Issue

Προηγμένος εντοπισμός απειλών σε endpoints και Servers

Είναι φανερό πλεόν, ότι οι στοχευμένες επιθέσεις και προηγμένες απειλές έχουν την ικανότητα να διαφεύγουν της προσοχής παραδοσιακών συστημάτων προστασίας και να δρουν ανενόχλητα αποσπώντας δεδομένα και πληροφορίες.

Οι κλασσικές συσκευές προστασίας από προηγμένες απειλές, εντοπίζουν τις ύποπτες κινήσεις σε επίπεδο δικτύου, αλλά δεν μπορούν να επιβεβαιώσουν αν υπάρχει διήθηση στο endpoint. Σίγουρα δεν έχουν την εγγενή δυνατότητα, να διερευνήσουν τις λεπτομέρειες και το εύρος της επίθεσης σε όλο το δίκτυο και οργανισμό.

Για τον λόγο αυτό η **Trend Micro** δημιούργησε τον **Endpoint Sensor** που προσαρμόζεται σε υπολογιστές και Server, εντός ή εκτός οργανισμού λειτουργώντας σαν άγρυπνος φρουρός. Πρόκειται για ένα προηγμένο εργαλείο που μέσω συνεχούς παρακολούθησης συμπεριφορών - πάντα σε σχέση με κανόνες ανίχνευσης - αποκτά επίγνωση μιας επικείμενης επίθεσης. Έρχεται στην ουσία να διευρύνει τη φιλοσοφία **«Connected Threat Defense»**, μια στρατηγική προσέγγιση προστασίας, που υιοθετεί η Trend Micro για όλα της τα προϊόντα.

Λειτουργεί επίσης, ως προηγμένο εργαλείο forensics καταγράφοντας και ενημερώνοντας σε λεπτομέρεια όλες τις κινήσεις σε επίπεδο λειτουργικού για γρήγορη αξιολόγηση της κατάστασης. Χρησιμοποιεί πληροφορίες από το **Trend Micro™ Deep Discovery™** συγκεκριμένα τα Indicators of Compromise (IOC) (Δείκτες Παραβίασης) και από άλλες πηγές, για να διενεργήσει πολύ-επίπεδη έρευνα σε όλα τα endpoints, τους χρήστες και τους servers.

Με αυτό τον τρόπο μπορούμε να πετύχουμε:

- Την επιβεβαίωση προειδοποιήσεων επίθεσης από το Trend Micro™ Deep Discovery™ Inspector ή άλλες λύσεις ασφάλειας
- Να εντοπίσουμε συγκεκριμένα Find IOCs, malware, ή κίνηση C&C
- Να αναλύσουμε πραγματικά το αποτέλεσμα της συμπεριφοράς ενός malware
- Να ανακαλύψουμε τα χαρακτηριστικά και το εύρος μιας επίθεσης

Βασικά Χαρακτηριστικά του Endpoint Sensor

- Πρόκειται για ένα **πολύ ελαφρύ client** που εγκαθίσταται στο ίδιο το Endpoint και καταγράφει σημαντικές κινήσεις και επικοινωνίες που γίνονται στο kernel level παρέχοντας λεπτομερή ιστορικό, που είναι διαθέσιμο σε πραγματικό χρόνο.
- Μπορούν να καθοριστούν **σύνθετοι παράμετροι αναζήτησης** στα Endpoints για συγκεκριμένες επικοινωνίες, malware, κινήσεις στο registry, σε λογαριασμούς, σε εργασίες που τρέχουν και πολλά άλλα ακόμη.
- Οι δυνατότητες συνεχούς παρακολούθησης αποκαλύ-

Αλεξία Χριστοφή
Managing Director CYSOFT
www.cysoft.gr

πτουν γνωστές και άγνωστες απειλές βάσει προκαθορισμένων κανόνων ή κανόνων OpenIOC. Μπορεί ακόμη να μας δώσει πληροφορίες για τις τακτικές που χρησιμοποιεί μια απειλή, τον τρόπο που είναι δομημένη ή ακόμη και η τεχνολογία που χρησιμοποιήθηκε για την εκτέλεσή της.

- Οι αναζητήσεις μπορούν να γίνουν μέσα στο ίδιο το Endpoint Sensor Manager ή με το Trend Micro™ Control Manager™—για να είμαστε σε θέση **να αντιδράσουμε άμεσα σε επιθέσεις** από το αποτέλεσμα που θα δώσουν τα IOC και ενημερώσεις από άλλα συστήματα.
- Η ανάλυση συσχετιζόμενων και συμφραζόμενων στοιχείων από διάφορα επίπεδα του δικτύου όπου χρησιμοποιεί διαδραστικούς πίνακες ενημέρωσης που **αναλύουν τα αποτελέσματα σε βάθος χρόνου** για όλο τον οργανισμό.
- Τα ύποπτα ψηφιακά αντικείμενα που θα ανακαλύψει το Endpoint Sensor συλλέγονται και αποστέλλονται στο Trend Micro™ Deep Discovery™ Analyzer για **λεπτομερή ανάλυση**.
- Παρακολουθεί, καταγράφει και ενημερώνει με λεπτομέρεια κινήσεις **σε επίπεδο λειτουργικού όλων των endpoint** (Windows-based servers, desktop και laptop) όπου και αν βρίσκονται, τοπικά, απομακρυσμένα ή cloud.
- Μπορεί να εγκατασταθεί και να **συνυπάρξει αρμονικά** με όλα τα συστήματα αντι-ιοτικής προστασίας σε οποιονδήποτε endpoint/server

4 βήματα εντοπισμού απειλών

1. Το Deep Discovery εντοπίζει στοχευμένες απειλές στο δίκτυο

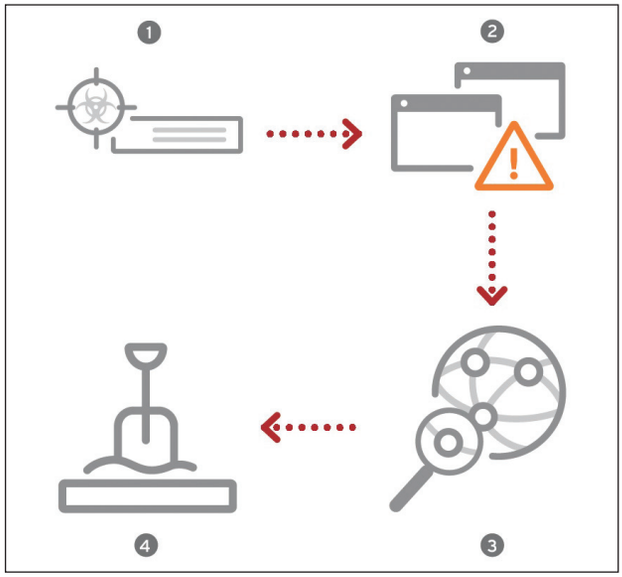
2. Στη συνέχεια, αποστέλλει τον Δείκτη Παραβιάσεων (IOC) στο Endpoint Sensor

3. ο Endpoint Sensor αναζητά πιθανή διήθηση και προσπαθεί να εντοπίσει παρόμοιους δείκτες απειλών, χαρτογραφώντας την εξέλιξη σε πραγματικό χρόνο.

4. Χρησιμοποιεί κανόνες έτοιμους ή παραμετροποιημένους για να παρακολουθεί συμπεριφορές στα Endpoint. Στην περίπτωση που εντοπίσει κάτι το στέλνει στο Deep Discovery Analyzer για sandboxing.

Πως ακριβώς λειτουργεί

Endpoint Sensor Agent – Τρέχει διακριτικά συλλέγοντας σε βάθος πληροφορίες από το σύστημα, που αποθηκεύονται και τακτοποιούνται για επεξεργασία από τον Endpoint Manager.



Μπορεί επίσης ο Agent να «φωτογραφήσει» σε πραγματικό χρόνο την κατάσταση της μνήμης και του registry.

Κεντρικός Έλεγχος & Διαχείριση – Ο κεντρικός server επικοινωνεί τα ευρήματά του στο Trend Micro Control Manager για περεταίρω επεξεργασία

Κριτήρια Έρευνας – Πολλαπλά επίπεδα αναζήτησης και εξακρίβωσης μπορούν να διεξαχθούν με διάφορες παραμέτρους π.χ. IP, Port, Domain, DNS, Malware (όνομα, τύπος αρχείου), κινήσεις στο registry, processes που τρέχουν ή χρήση account.

Παρακολούθηση Συμπεριφοράς – Χρησιμοποιώντας προκαθορισμένους ή/και παραμετροποιημένους κανόνες IOC παρακολουθεί συμπεριφορές και συσχετισμούς για να εντοπίσει επιθέσεις.

Συλλογή Υπόπτων Αντικειμένων – Ύποπτα ψηφιακά αντικείμενα και επισυνάψεις περνούν αυτόματα στο κεντρικό sandbox του Deep Discovery για περαιτέρω έρευνα.

Έρευνα και Αποτελέσματα – Ο Endpoint Sensor προσφέρει μια πλούσια συλλογή από πληροφορίες σε βάθος χρόνο και λεπτομερή εικόνα για την κατάσταση ενός δικτύου. Οι πληροφορίες αυτές μπορούν να αξιοποιηθούν για περεταίρω έρευνα. Περιλαμβάνει χρονογραφημένο χάρτη της κίνησης στο δίκτυο, λεπτομερή εικόνα της προετοιμασίας μιας επίθεσης, εντοπισμό κακόβουλων αντικειμένων, διαδικασιών και έλεγχο όλων των endpoint του οργανισμού βάσει ευρημάτων.

Για περισσότερες πληροφορίες για το Endpoint Sensor και για το πως δένει με άλλα προϊόντα της όπως την σειρά Deep Discovery και Trend Micro Control Manager επικοινωνήστε μαζί μας. **(www.cysoft.gr)** ITSecurity