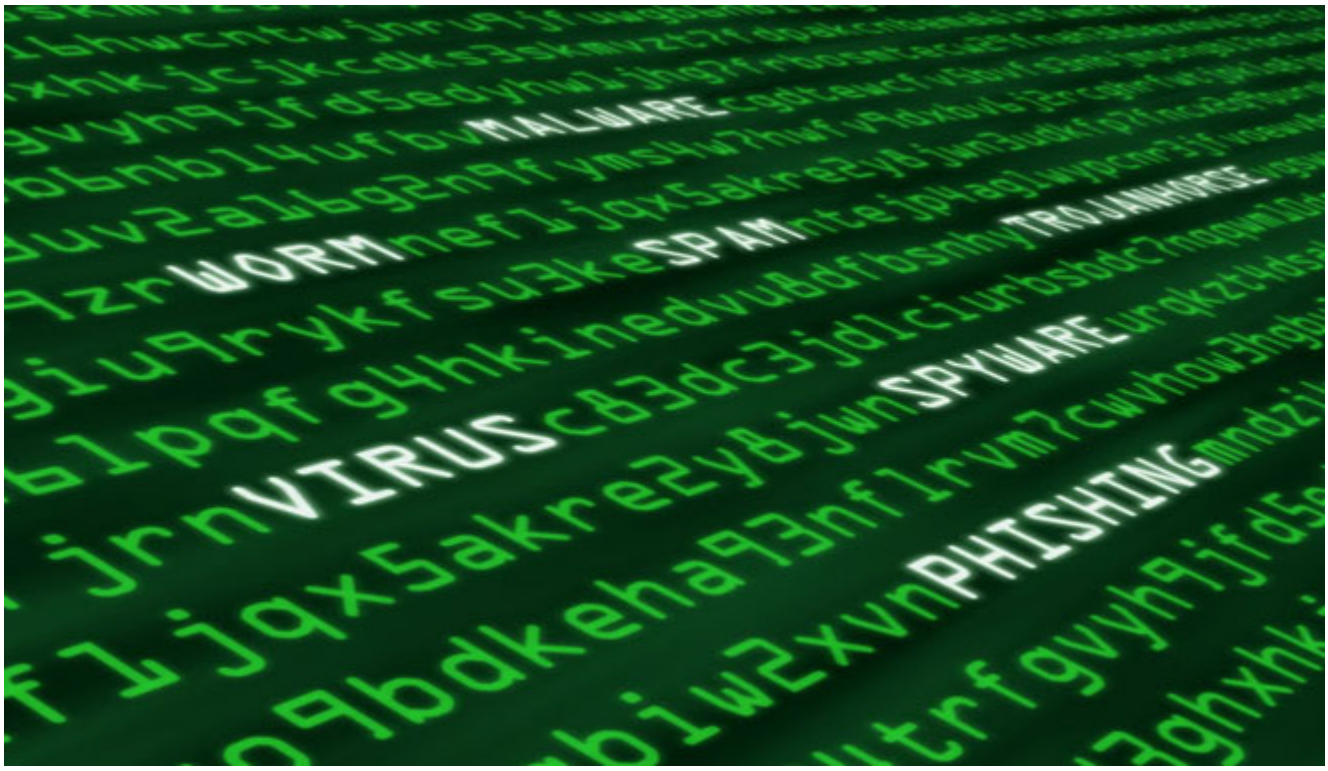
9 Φεβρουαρίου 2017

Hacking σε 40 χώρες με κρυμμένο malware

/ Πεμπτουσία

Image not found or type unknown



Τράπεζες, εταιρείες τηλεπικοινωνιών και κυβερνητικοί οργανισμοί στις ΗΠΑ, τη Νότια Αμερική, την Ευρώπη και την Αφρική βρίσκονται μεταξύ των κορυφαίων στόχων, με τις διαβόητες ομάδες GCMAN και Carbanak να περιλαμβάνονται στους βασικούς υπόπτους.

Οι ειδικοί της Kaspersky Lab ανακάλυψαν μια σειρά από «αόρατες» στοχευμένες επιθέσεις που χρησιμοποιούν μόνο νόμιμο λογισμικό: ευρέως διαθέσιμα εργαλεία για δοκιμές διείσδυσης και εργαλεία διαχείρισης, καθώς και το πλαίσιο συνεργασίας PowerShell για την αυτοματοποίηση εργασιών στα Windows – με κανένα αρχείο κακόβουλου λογισμικού να βρίσκεται στον σκληρό δίσκο, αλλά να κρύβεται στη μνήμη. Αυτή η συνδυασμένη προσέγγιση βοηθά στην αποφυγή του εντοπισμού από τεχνολογίες whitelisting και αφήνει τους ερευνητές σχεδόν χωρίς αντικείμενα ή δείγματα κακόβουλου λογισμικού με τα οποία θα μπορούσαν να εργαστούν.

Οι επιτιθέμενοι παραμένουν στο σύστημα για αρκετό χρονικό διάστημα με στόχο να συγκεντρώσουν πληροφορίες πριν τα ίχνη τους εξαφανιστούν από αυτό έπειτα από την πρώτη επανεκκίνηση.

Στο τέλη του 2016, τράπεζες ήρθαν σε επαφή με ειδικούς της Kaspersky Lab στο CIS, οι οποίοι εντόπισαν το Meterpreter (λογισμικό για δοκιμές διείσδυσης που σήμερα χρησιμοποιείται συχνά για κακόβουλους σκοπούς) στη μνήμη των servers τους σε χρονικές στιγμές που υποτίθεται ότι δεν θα έπρεπε να είναι εκεί. Η Kaspersky Lab ανακάλυψε ότι ο κώδικας του Meterpreter συνδυάστηκε με μια σειρά από νόμιμα σενάρια του PowerShell και άλλα βοηθητικά προγράμματα. Τα συνδυασμένα εργαλεία είχαν προσαρμοστεί σε κακόβουλο κώδικα που θα μπορούσε να κρυφτεί στη μνήμη, συλλέγοντας αόρατα τους κωδικούς πρόσβασης των διαχειριστών του συστήματος, έτσι ώστε οι επιτιθέμενοι θα ήταν σε θέση να ελέγχουν από απόσταση τα συστήματα του θύματος. Ο τελικός στόχος φαίνεται να ήταν η πρόσβαση σε οικονομικές διαδικασίες.

Η Kaspersky Lab έκτοτε αποκάλυψε ότι οι επιθέσεις αυτές συμβαίνουν σε μαζική κλίμακα: πλήγματα σε πάνω από 140 δίκτυα επιχειρήσεων σε διάφορους επιχειρηματικούς τομείς, με τα περισσότερα θύματα να βρίσκονται στις ΗΠΑ, τη Γαλλία, τον Ισημερινό, την Κένυα, το Ηνωμένο Βασίλειο και τη Ρωσία.

Η γεωγραφία των οργανισμών που δέχτηκαν επίθεση με τη μέθοδο που ανακαλύφθηκε

Συνολικά, έχουν καταγραφεί «μολύνσεις» σε 40 χώρες.

Δεν είναι ακόμα γνωστό ποιος βρίσκεται πίσω από τις επιθέσεις. Η χρήση ανοιχτού κώδικα εκμετάλλευσης αδυναμιών, κοινών βοηθητικών προγραμμάτων των Windows και άγνωστων περιοχών καθιστούν σχεδόν αδύνατο να προσδιοριστεί η ομάδα που ήταν υπεύθυνη – ή ακόμα και αν πρόκειται για μια ενιαία ομάδα ή περισσότερες ομάδες που μοιράζονται τα ίδια εργαλεία. Γνωστές ομάδες που έχουν τις περισσότερες παρόμοιες προσεγγίσεις είναι οι GCMAN και Carbanak.

Τέτοια εργαλεία καθιστούν επίσης πιο δύσκολη την αποκάλυψη των λεπτομέρειών της επίθεσης. Η συνηθισμένη διαδικασία που ακολουθείται κατά την αντιμετώπιση περιστατικών είναι ένας ερευνητής να ακολουθήσει τα ίχνη και τα δείγματα που αφήνονται στο δίκτυο από τους επιτιθέμενους. Και ενώ τα δεδομένα στο σκληρό δίσκο μπορούν να παραμένουν διαθέσιμα για ένα χρόνο μετά το γεγονός, αντικείμενα που κρύβονται στη μνήμη θα σβηστούν με την πρώτη επανεκκίνηση του υπολογιστή. Ευτυχώς, στην περίπτωση αυτή, οι ειδικοί έφτασαν σε αυτά έγκαιρα.

«Η αποφασιστικότητα των επιτιθέμενων να κρύψουν τη δραστηριότητά τους και να κάνουν την ανίχνευση και την αντιμετώπιση των περιστατικών όλο και πιο δύσκολη εξηγεί την τελευταία τάση των αντι-εγκληματολογικών τεχνικών και των κακόβουλων λογισμικών που βασίζονται στη μνήμη των συσκευών. Αυτός είναι ο λόγος που η εγκληματολογική έρευνα σχετικά με την μνήμη καθίσταται κρίσιμη για την ανάλυση κακόβουλου λογισμικού και των λειτουργιών του. Σε αυτά τα συγκεκριμένα περιστατικά, οι επιτιθέμενοι χρησιμοποίησαν κάθε δυνατή αντι-εγκληματολογική τεχνική, αποδεικνύοντας πως δεν υπάρχουν αρχεία κακόβουλου λογισμικού που απαιτούνται για την επιτυχημένη εκδιήθηση των δεδομένων από ένα δίκτυο, και πώς η χρήση νόμιμων και ανοικτού κώδικα βοηθητικών προγραμμάτων καθιστά την απόδοση σχεδόν αδύνατη», δήλωσε ο Sergey Golovanov, Principal Security Researcher της Kaspersky Lab.

Οι επιτιθέμενοι είναι ακόμα ενεργοί, για αυτό είναι σημαντικό να σημειωθεί ότι η ανίχνευση μιας τέτοιας επίθεσης είναι πιθανή μόνο στη μνήμη RAM, το δίκτυο και το μητρώο – και ότι, σε τέτοιες περιπτώσεις, η χρήση των κανόνων Yara με βάση τη σάρωση κακόβουλων αρχείων δεν έχουν καμία χρήση.

Λεπτομέρειες σχετικά με το δεύτερο μέρος της λειτουργίας, που δείχνει πώς οι επιτιθέμενοι εφαρμόζουν μοναδικές τακτικές για να αποσύρουν τα χρήματα μέσω ATM θα παρουσιάσουν ο Sergey Golovanov και Igor Soumenkov στο Security Analyst Summit, που θα πραγματοποιηθεί από 2 έως 6 Απριλίου 2017.

Τα προϊόντα της Kaspersky Lab εντοπίζουν λειτουργίες χρησιμοποιώντας τις παραπάνω τακτικές, τεχνικές και διαδικασίες. Περισσότερες πληροφορίες σχετικά με αυτήν την ιστορία και τους κανόνες Yara για την εγκληματολογική ανάλυση μπορείτε να βρείτε στο ειδικό blog στον ιστότοπο Securelist.com. Τεχνικές λεπτομέρειες, συμπεριλαμβανομένου των Δεικτών Συμβιβασμού επίσης παρέχονται στους πελάτες της των of Kaspersky Intelligence Services.

Πηγή: secnews.gr