Η ESET κερδίζει την εμπιστοσύνη των αναγνωστών του Computer Bild

Το ESET Smart Security 9 επιλέχτηκε από τους αναγνώστες του μεγαλύτερου IT περιοδικού της Ευρώπης ως η καλύτερη λύση ασφάλειας για οικιακούς χρήστες

Η ESET® πέτυχε μία σημαντική νίκη στη Γερμανία, με τη λύση ESET Smart Security 9 να λαμβάνει το βραβείο «*Golden Computer*» για το καλύτερο προϊόν στην κατηγορία: ασφάλεια για οικιακούς χρήστες, καθώς αποτέλεσε την πρώτη επιλογή των αναγνωστών του γερμανικού Computer Bild, του μεγαλύτερου IT περιοδικού της Ευρώπης.

Η τελετή απονομής των βραβείων πραγματοποιήθηκε την πρώτη εβδομάδα του Σεπτεμβρίου, πριν την IFA – την κορυφαία εμπορική έκθεση για ηλεκτρονικά είδη και οικιακές συσκευές για καταναλωτές που πραγματοποιήθηκε στο Βερολίνο.

Το Computer Bild αποτελεί το μεγαλύτερο περιοδικό για υπολογιστές, όχι μόνο στη Γερμανία, αλλά και σε όλη την Ευρώπη. Όπως σχετικά αναφέρεται στο αφιέρωμά του για τα βραβεία «Golden Computer»: «*Οι επαγγελματίες της ασφάλειας από την ESET απέσπασαν το πολυπόθητο τρόπαιο «Golden Computer». Κέρδισαν στην κατηγορία ασφαλείας με το λογισμικό ESET Smart Security 9.*»

«Μας τιμά και ταυτόχρονα μας ευχαριστεί ιδιαίτερα αυτή η αναγνώριση από τους Γερμανούς χρήστες μας – τους αναγνώστες του Computer Bild. Αποτελεί ένα σημαντικό κίνητρο για να συνεχίσουμε τη βασικά μας αποστολή: την προστασία των χρηστών από τις απειλές στον κυβερνοχώρο», δήλωσε ο Miro Mikus, EMEA Sales and Marketing Director της ESET.

Νωρίτερα κατά τη διάρκεια του έτους, η λύση ESET Smart Security 9 κέρδισε στις αυστηρές δοκιμές του Computer Bild, τερματίζοντας στην πρώτη θέση ανάμεσα στα 13 προϊόντα για καταναλωτές που συμμετείχαν στο Internet Security Test του περιοδικού, εξασφαλίζοντας την καλύτερη βαθμολογία.

Σύντομα, η ESET θα κυκλοφορήσει την έκδοση των προϊόντων ασφάλειας για καταναλωτές για το 2017, συμπεριλαμβανομένης της λύσης ESET Smart Security 10.

Αναβάθμιση της δωρεάν εφαρμογής ESET Online Scanner

Η ESET® ανακοίνωσε τη διάθεση μίας νέας έκδοσης του ESET Online Scanner – της δωρεάν εφαρμογής της που βασίζεται στην τεχνολογία ThreatSense® για σάρωση και αφαίρεση του κακόβουλου λογισμικού, προσφέροντας πλήρεις σαρώσεις antivirus μέσω του προγράμματος περιήγησης διαδικτύου.

Η νέα αυτή έκδοση του ESET on-line Scanner λειτουργεί ανεξαρτήτως του προγράμματος περιήγησης, που σημαίνει ότι εύκολα μπορεί να εκτελεστεί από όλα τα γνωστά προγράμματα περιήγησης στο Web. Επιπλέον, η εγκατάσταση είναι πλέον δυνατή χωρίς να χρειάζονται δικαιώματα διαχειριστή, γεγονός που καθιστά τη σάρωση και την αφαίρεση του κακόβουλου λογισμικού από τους ηλεκτρονικούς υπολογιστές ακόμα πιο απλή.

Σχεδιασμένο να είναι φιλικό προς το χρήστη, το ESET Online Scanner περιλαμβάνει επίσης και κάποιες πρόσθετες λειτουργίες για την αφαίρεση του κακόβουλου λογισμικού,όπως:

· **Σάρωση σε περιοχές Autostart** – Επιτρέπει τη σάρωση σε περιοχές Autostart αλλά και στον Boot sector για κρυμμένες απειλές – απλά επιλέγοντας τη συγκεκριμένη λειτουργία στο «advanced setup/scan targets»

· **Αρχείο αφαίρεσης κακόβουλο λογισμικού** – Αφαιρεί κακόβουλο κώδικα που βρίσκεται αποκλειστικά στο αρχείο συστήματος (registry)

· **Καθαρισμός κατά την επανεκκίνηση που ακολουθείται από επανάληψη σάρωσης** – Αν χρειαστεί, το ESET Online Scanner μπορεί να αφαιρέσει το πιο επίμονο malware με αυτόματο καθαρισμό μετά από επανεκκίνηση

Για περισσότερες πληροφορίες σχετικά με τη δωρεάν εφαρμογή ESET Online Scanner οι ενδιαφερόμενοι μπορούν να επισκεφτούν τη σελίδα ESET Knowledgebase ή να την «τρέξουν» απευθείας από τη σελίδα Eset.com

Η ESET στο London Gartner Summit

Η ESET® συμμετέχει στο Gartner Security & Risk Management summit που πραγματοποιείται αυτό το Σεπτέμβριο στο Λονδίνο. Με τη συμμετοχή κορυφαίων στελεχών της, η ESET θα παρουσιάσει την τελευταία λέξη της τεχνολογίας για τις επιχειρήσεις και τις πιο πρόσφατες απειλές στον κυβερνοχώρο, όπως τη ραγδαία άνοδο των ransomware, ενώ θα συζητηθούν θέματα πολιτικής που συνδέονται με τη βιομηχανία – ειδικά τους κανονισμούς προστασίας προσωπικών δεδομένων και κρυπτογράφησης στην Ευρωπαϊκή Ένωση.

Ένα από τα σημαντικά θέματα που θα συζητηθούν είναι η ταχεία ανάπτυξη της κρυπτογράφησης ransomware, για την καταπολέμηση του οποίου η ESET επενδύει πόρους στην ανίχνευση και πραγματοποιεί εκτεταμένη έρευνα. *«Ένας πραγματικός μπελάς αυτές τις μέρες είναι το ransomware, κυρίως επειδή τα συμπτώματά του είναι τόσο ορατά και οι επιπτώσεις πολύ άμεσες. Πολλοί χρήστες δεν προστατεύουν τον εαυτό τους σωστά και δεν δίνουν αρκετή προσοχή στην υπεύθυνη online συμπεριφορά»*, λέει ο Chief Research Officer της ESET, Juraj Malcho, ο οποίος θα παρευρίσκεται στο Gartner Summit.

Το άλλο σημαντικό θέμα στην κορυφή της ατζέντας θα είναι η νομοθεσία για την προστασία του απορρήτου των δεδομένων στην ΕΕ. *«Η προστασία των δεδομένων αποτελεί ένα βασικό στοιχείο των κανονισμών της ΕΕ, γεγονός που καθιστά υποχρεωτικό για τις επιχειρήσεις το να προστατεύουν επαρκώς τα προσωπικά δεδομένα.*

Οι λύσεις και η τεχνολογία της ESET είναι κατάλληλα εξοπλισμένες για την αντιμετώπιση των βασικών πτυχών του κανονισμού – συγκεκριμένα τεχνικά μέτρα που διασφαλίζουν την ασφάλεια, την ακεραιότητα και την εμπιστευτικότητα των προσωπικών δεδομένων μέσω κρυπτογράφησης, πιστοποίησης και προϊόντων προστασίας endpoint», λέει Palo Μπαλάι, Head of ESET EMEA Business Development. Περισσότερες πληροφορίες σχετικά με αυτούς τους κανονισμούς της ΕΕ και την τεχνολογία της ESET, όπως το DESlock, είναι διαθέσιμες στο σχετικό ειδικό white paper. Επίσης, οι Palo Balaj και Juraj Malcho της ESET θα είναι διαθέσιμοι για τους συμμετέχοντες που επιθυμούν να κανονίσουν συναντήσεις για πληρέστερη ενημέρωση.

Το Gartner Summit θα πραγματοποιηθεί στο Λονδίνο, 12 – 13 Σεπτεμβρίου 2016 στο ξενοδοχείο O2 London InterContinental. Η ESET προσκαλεί όλους τους συμμετέχοντες να επισκεφθούν το περίπτερο της, επικοινωνώντας μέσω της ειδικά διαμορφωμένης σελίδας, της αντίστοιχης τοπικής επαφής ή μέσω του ESET EMEA PR. Οι εκπρόσωποι των ΜΜΕ παρακαλούνται να επικοινωνήσουν με το Ευρωπαϊκό Γραφείο Τύπου της Gartner.

Οι ερευνητές της ESET εντόπισαν updates του crypto-

ransomware TorrentLocker

Το TorrentLocker, που η ESET είχε αναλύσει το 2014, εξακολουθεί να είναι ενεργό, και, χάρη στον τρόπο επιλογής των υποψήφιων θυμάτων με στοχευμένα spam, αποφεύγει την προσοχή που λαμβάνουν τα πιο γνωστά crypto-ransomware. Ωστόσο, οι ερευνητές της ESET εξακολουθούν να παρακολουθούν το συγκεκριμένο κακόβουλο λογισμικό.

«*Η συμμορία πίσω από TorrentLocker φαίνεται ότι εξακολουθεί να είναι στο παιχνίδι. Έχουν βελτιώσει την τακτική τους και έχουν ανανεώσει σιγά-σιγά αυτό το ransomware, προσπαθώντας να το διατηρούν μη ανιχνεύσιμο*» λέει ο Marc-Etienne M. Léveillé, ερευνητής malware της ESET.

Το TorrentLocker εξαπλώνεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου με μια σελίδα που υποστηρίζει ότι πρέπει να γίνει λήψη ενός «εγγράφου» (υποτίθεται ότι πρόκειται για τιμολόγιο ή αρχείο με κωδικό εντοπισμού). Αν γίνει λήψη του κακόβουλου «εγγράφου» και ανοιχτεί από το χρήστη, το TorrentLocker εκτελείται. Ξεκινά την επικοινωνία του με το C&C server και κρυπτογραφεί τα αρχεία του θύματος.

Ένα πολύ γνωστό χαρακτηριστικό του TorrentLocker είναι το πόσο τοπικά εστιασμένες είναι οι λειτουργίες της λήψης, των λύτρων και των σελίδων πληρωμής. Στα θύματα παρέχονται πληροφορίες στη δική τους γλώσσα και στο τοπικό τους νόμισμα.

Οι βελτιώσεις στο TorrentLocker ξεπερνούν τους μηχανισμούς προστασίας των χρηστών του διαδικτύου σε επιλεγμένες χώρες, δηλαδή οι τρόποι επικοινωνίας του TorrentLocker με τους διακομιστές Command-and-Control, η προστασία του C&C server με ένα επιπλέον στρώμα κρυπτογράφησης, οι τεχνικές αποφυγής του εντοπισμού και η διαδικασία κρυπτογράφησης των αρχείων των χρηστών.

Ένα από τα σημαντικότερα βελτιωμένα χαρακτηριστικά του CryptoLocker είναι η προσθήκη ενός script στην αλυσίδα που

οδηγεί στο τελικό κακόβουλο εκτελέσιμο αρχείο.

«Ο σύνδεσμος στο spam μήνυμα ηλεκτρονικού ταχυδρομείου οδηγεί σε ένα PHP script που φιλοξενείται σε ένα παραβιασμένο διακομιστή. Αυτό το script ελέγχει αν ο επισκέπτης περιηγείται στη στοχευμένη χώρα και, αν ναι, θα εμφανιστεί η σελίδα με το επόμενο στάδιο αυτού του κακόβουλου λογισμικού. Σε αντίθετη περίπτωση, ο επισκέπτης ανακατευθύνεται στην Google» εξηγεί ο Marc-Etienne M. Léveillé.

Στην ανάλυση αυτού του κακόβουλου λογισμικού και των εκστρατειών του, οι ερευνητές της ESET διαπίστωσαν ότι 22 χώρες έλαβαν μια μεταφρασμένη έκδοση της σελίδας για λύτρα ή για πληρωμή. Ωστόσο, 7 από αυτές δεν έχουν πληγεί μέχρι στιγμής από οποιαδήποτε σημαντική εκστρατεία spam TorrentLocker. Πρόκειται για τη Γαλλία, την Ιαπωνία, τη Μαρτινίκα, την Πορτογαλία, τη Δημοκρατία της Κορέας, την Ταϊβάν και την Ταϊλάνδη.

Λεπτομέρειες σχετικά με τις βελτιώσεις στο crypto-malware TorrentLocker είναι διαθέσιμες στο αναλυτικό άρθρο στο επίσημο blog της ESET, WeLiveSecurity.

Οι ενδιαφερόμενοι μπορούν επίσης να βρουν συμβουλές της ESET για την προστασία από ransomware στο άρθρο «11 things you can do to protect against ransomware».

Μερικοί χρήσιμοι κανόνες από την ESET για τη δημιουργία ισχυρών passwords

Οι κίνδυνοι που παραμονεύουν στον εικονικό κόσμο του διαδικτύου πολλές φορές δεν γίνονται αντιληπτοί σε μερικούς χρήστες, που έχουν μεγαλώσει στην εποχή που δεν υπήρχε Internet και κοινωνικά δίκτυα, σε αντίθεση με τις νέες γενιές που μεγαλώνουν στην ψηφιακή εποχή και είναι πιο υποψιασμένες. Θέλοντας να βοηθήσει τους ανυποψίαστους χρήστες, ο Ondrej Kubovic, IT Security Specialist της ESET, προσφέρει μερικούς βασικούς κανόνες για ασφαλή passwords.

1. Δημιουργήστε ένα μοναδικό κωδικό πρόσβασης για κάθε λογαριασμό και μην το μοιραστείτε με κανέναν.
2. Ο κανόνας είναι – όσο μεγαλύτερος ο κωδικός πρόσβασης, τόσο πιο ασφαλής. Ξεκινήστε με τουλάχιστον 8 χαρακτήρες, αλλά επιμηκύνετε τον κωδικό αν χρησιμεύει για να προστατεύει πολύτιμα δεδομένα ή λογαριασμούς. Αν έχετε πρόβλημα να θυμηθείτε ένα σύνθετο κωδικό πρόσβασης, μπορείτε επίσης να επιλέξετε μια συνθηματική φράση ή να χρησιμοποιήσετε έναν password manager (αναλύονται παρακάτω)
3. Αποφύγετε κοινές λέξεις, ονόματα, ημερομηνίες, αριθμούς ή προφανείς επιλογές, όπως 12345678, password ή qwerty.
4. Προσθέστε ένα ψηφιακό κομμάτι, όπως αριθμούς και ειδικούς χαρακτήρες (@, #,!, κλπ), ή χρησιμοποιήστε τα αντικαθιστώντας κάποια από τα γράμματα στον κωδικό πρόσβασής σας.
5. Εάν επιλέξετε την αντικατάσταση, προσπαθήστε να μην χρησιμοποιήσετε τις συνήθεις «ανορθογραφίες», όπως αντικατάσταση του «α» με «@» ή «ι» με «1» ή «!».
6. Αλλάξτε τακτικά τους κωδικούς πρόσβασής. Και εδώ ισχύει

ότι όσο πιο σημαντικά τα δεδομένα που προστατεύονται, τόσο πιο σύντομα πρέπει να αλλάζουν οι κωδικοί.

7. Ένας από τους σημαντικότερους κανόνες είναι να μην χρησιμοποιήσετε ξανά τον ίδιο κωδικό πρόσβασης σε άλλους λογαριασμούς. Με αυτόν τον τρόπο, αν κλαπεί, κινδυνεύει μόνο ένας λογαριασμός, και αξίζει να το επισημαίνουμε ακόμη κι αν επαναλαμβανόμαστε.

Στη θεωρία μπορεί να ακούγεται αρκετά απλό, αλλά η πραγματικότητα είναι πιο σύνθετη. Πολλαπλές μελέτες έχουν δείξει ότι ο μέσος χρήστης έχει δεκάδες κωδικούς πρόσβασης για έναν ακόμη μεγαλύτερο αριθμό λογαριασμών, γεγονός που δυσχεραίνει τη διαχείρισή τους. Ωστόσο, υπάρχουν στρατηγικές για να παραμείνετε ασφαλείς διευκολύνοντας τη διαδικασία. Το πρώτο πράγμα που μπορεί να βοηθήσει είναι οι συνθηματικές φράσεις, ή αλλιώς passphrases, που παρόλου που είναι μεγαλύτερες από τους κωδικούς πρόσβασης, είναι πιο εύκολο να απομνημονευτούν. Ένας άλλος τρόπος είναι η χρήση ενός αξιόπιστου password manager, που αποθηκεύει όλους τους κωδικούς σε ένα μέρος, και το μόνο που χρειάζεται να θυμάται ο χρήστης είναι ένα από αυτά, εκείνο δηλαδή που θα του επιτρέψει να ξεκλειδώσει την εφαρμογή.

Η ESET ανακάλυψε το πρώτο

botnet σε Android που ελέγχεται μέσω Twitter

Οι ερευνητές της ESET ανακάλυψαν ένα backdoor Trojan που επιτίθεται σε Android το οποίο ελέγχεται μέσω tweets. Ανιχνεύεται από την ESET ως Android/Twitoor, και είναι η πρώτη κακόβουλη εφαρμογή που χρησιμοποιεί το Twitter αντί του παραδοσιακού διακομιστή C&C (command-and-control).

Αφού ξεκινήσει, το Trojan κρύβει την παρουσία του στο σύστημα και ελέγχει τον καθορισμένο λογαριασμό Twitter σε τακτά χρονικά διαστήματα για εντολές. Με βάση τις λαμβανόμενες εντολές, μπορεί είτε να κατεβάσει κακόβουλες εφαρμογές ή να αλλάξει το C&C λογαριασμό Twitter σε ένα άλλο.

«Η χρήση του Twitter για τον έλεγχο ενός botnet είναι ένα καινοτόμο βήμα για την πλατφόρμα Android» επισημαίνει ο Lukáš Štefanko, ο ερευνητής malware της ESET που ανακάλυψε την κακόβουλη εφαρμογή.

Σύμφωνα με τον Štefanko, τα κανάλια επικοινωνίας που βασίζονται στα κοινωνικά δίκτυα είναι δύσκολο να εντοπιστούν και αδύνατον να εμποδιστουν πλήρως, ενώ ταυτόχρονα είναι εξαιρετικά εύκολο για τους απατεώνες να ανακατευθύνουν εκ νέου την επικοινωνία σε άλλο λογαριασμό.

Το Twitter χρησιμοποιήθηκε για πρώτη φορά για τον έλεγχο botnets των Windows το 2009. *«Σχετικά με το χώρο των Android, αυτό το μέσο απόκρυψης είχε παραμείνει ανεκμετάλλευτο μέχρι τώρα. Στο μέλλον, όμως statuses, μπορούμε να αναμένουμε ότι οι «κακοί» θα προσπαθήσουν να κάνουν χρήση των Facebook status ή να εκμεταλλευτούν το LinkedIn και άλλα κοινωνικά δίκτυα»*, προβλέπει ο Štefanko.

Το Android / Twitoor είναι ενεργό από τον Ιούλιο του 2016. Δεν μπορεί να βρεθεί σε οποιοδήποτε επίσημο κατάστημα εφαρμογών Android – σύμφωνα με τον Štefanko– αλλά μάλλον εξαπλώνεται

μέσω SMS ή μέσω κακόβουλων URL. Υποδύεται μια εφαρμογή porn player ή εφαρμογή MMS αλλά χωρίς την λειτουργικότητα. Αντ' αυτού, κατεβάζει διάφορες εκδόσεις κακόβουλου λογισμικού για mobile banking. Ωστόσο, αυτοί που διαχειρίζονται το botnet μπορούν να ξεκινήσουν τη διάδοση και άλλων κακόβουλων προγραμμάτων ανά πάσα στιγμή, συμπεριλαμβανομένου και ransomware, σύμφωνα με το Štefanko.

«Το Twitoor αποτελεί ένα άλλο παράδειγμα του ότι οι εγκληματίες του κυβερνοχώρου συνεχώς καινοτομούν. Οι χρήστες του Διαδικτύου θα πρέπει να διατηρούν ασφαλείς τις δραστηριότητές τους με καλές λύσεις ασφάλειας τόσο για υπολογιστές όσο και για φορητές συσκευές», καταλήγει ο Lukáš Štefanko.

Περισσότερες πληροφορίες στο σχετικό blogpost στο blog της ESET, WeLiveSecurity.

Διακρίσεις για την ESET στις συγκριτικές δοκιμές του Virus Bulletin

Στην συγκριτική έκθεση VBSpam για τον Ιούνιο του οργανισμού Virus Bulletin, επιβεβαιώνεται ξανά ότι η λύση ESET Mail Security για Microsoft Exchange Server αποτελεί την κορυφαία επιλογή στην αγορά αναφορικά με το φιλτράρισμα των spam,

αποσπώντας τη δεύτερη συνεχόμενη διάκριση VBSpam+. Στην 44η δοκιμή VBSpam Comparative, η λύση ESET Mail Security για Microsoft Exchange Server σημείωσε βαθμολογία 99,999 με μηδενικά false positives.

Παράλληλα, ο ανεξάρτητος οργανισμός Virus Bulletin δημοσίευσε άλλες δύο συγκριτικές εκθέσεις VB100, σχετικά με τον SUSE Linux Enterprise Server και τα Windows 8.1 Pro 64-Bit. Στη συγκριτική δοκιμή για SUSE Linux Enterprise Server, ο Virus Bulletin αξιολόγησε τη λύση ESET Endpoint Security for Linux, η οποία πέτυχε βαθμολογία 100% και στις δύο περιπτώσεις σάρωσης – on demand και on access. Ανάλογη βαθμολογία σημείωσε και η λύση ESET NOD32 Antivirus 9 στη δεύτερη συγκριτική δοκιμή, όπου τα Windows 8.1 αποτέλεσαν την πλατφόρμα δοκιμών.

«Τον τελευταίο καιρό, η λύση της ESET στις δοκιμές VBSpam Comparatives σημειώνει μία από τις καλύτερες επιδόσεις με πολύ ισχυρά αποτελέσματα. Συνολικά, μια μακρά ιστορία εξαιρετικής απόδοσης και μηδενικών false positives, αποτελεί σαφή ένδειξη ενός αξιόπιστου προϊόντος για φιλτράρισμα spam στις επιχειρήσεις», δήλωσε ο Martijn Grooten, εκδότης της έκθεσης Virus Bulletin.» Από την πλευρά του, ο John Hawes, Chief of Operations του Virus Bulletin, σημείωσε ότι «*Η ESET συμμετείχε και στις δύο δοκιμές με δύο χαρακτηριστικά που αποτελούν σήμα κατατεθέν της: χαμηλό αποτύπωμα και ισχυρή ανίχνευση, προσθέτοντας δύο ακόμη βραβεία VB100 στην τεράστια συλλογή της».*

«Η ESET συνεχίζει να δίνει σημαντική θέση στην προστασία από ανεπιθύμητα μηνύματα στην πολυεπίπεδη προσέγγισή της για την ασφάλεια επόμενης γενιάς. Κρατώντας το ποσοστό ανίχνευσης ανεπιθύμητων μηνυμάτων στο υψηλότερο δυνατό επίπεδο και τα false positives στο μηδέν, σημαίνει ότι είμαστε στο σωστό δρόμο για ακόμη πιο ασφαλή τεχνολογία» σχολιάζει ο Palo Luka, Chief Technology Officer στην ESET.

Περισσότερες πληροφορίες για τις λύσεις ESET στη σελίδα www.eset.com/gr.

Άριστες επιδόσεις για την ESET στις δοκιμές του VB100 σε Windows 10 Pro 64-bit

Ο ανεξάρτητος οργανισμός Virus Bulletin δημοσίευσε την πρώτη συγκριτική έκθεση προϊόντων που απευθύνονται σε επιχειρήσεις και απλούς χρήστες σε Windows 10 Pro 64-bit. Σύμφωνα με τα αποτελέσματα, η λύση ESET NOD32 Antivirus καταδεικνύεται ως η πιο αξιόπιστη διατηρώντας τον χαρακτηρισμό «most reliable performer» στον τομέα των χρηστών, αποσπώντας το 95ο βραβείο VB100.

Από το σύνολο των 24 λύσεων για απλούς χρήστες που συμμετείχαν στις δοκιμές του Virus Bulletin σε όλα τα επίπεδα, το ESET NOD32 Antivirus συνέχισε να παρουσιάζει άριστες επιδόσεις, καταγράφοντας μηδενικά false positives και πετυχαίνοντας για μία ακόμη φορά την αναγνώριση «Solid» για την εξαιρετική σταθερότητά του.

«Η ESET παραμένει η εταιρία με τις πιο αξιόπιστες επιδόσεις όλα αυτά τα χρόνια. Με πολύ ισχυρή ανίχνευση, μικρές πτώσεις στην πρόληψη αλλά εξαιρετική στην απόκριση, και με μια άψογη λειτουργία στις πιστοποιήσεις, η ESET προσθέτει ένα ακόμη βραβείο VB100 στην τεράστια συλλογή της» δήλωσε ο John Hawes, Chief of Operations του Virus Bulletin.

Στις συγκριτικές δοκιμές σε Windows 10, ο Virus Bulletin αναφέρει επίσης ότι το ESET NOD32 απέδειξε το χαμηλό αποτύπωμα στα εξαιρετικά αποτελέσματα επιδόσεων αναφορικά με τη χρήση σε RAM και CPU, σε συνδυασμό με γρήγορο χρόνο φόρτωσης.

«Το ESET NOD32 Antivirus συνεχίζει να τηρεί τις υποσχέσεις του για μία ελαφριά, σταθερή και φιλική προς το χρήστη πλατφόρμα, ακόμη και με Windows 10. Με αυτή την πρώτη δοκιμή, μπορούμε να έχουμε εμπιστοσύνη ότι παραμένουμε στην κορυφή των λύσεων προστασίας για απλούς χρήστες», είπε ο Eduard Kesely, Senior Product Manager της ESET.

Για περισσότερες πληροφορίες, επισκεφθείτε τη σελίδα www.eset.com/gr ή κατεβάστε την συγκριτική έκθεση Virus Bulletin VB100.

Το Nymaim εμφανίζεται πάλι σε Ευρώπη και Βόρεια Αμερική, φτάνοντας μέχρι τη Βραζιλία

Από την ανίχνευση του πρώτου κρούσματος Nymaim το 2013, έχουν καταγραφεί πάνω από 2,8 εκατομμύρια περιπτώσεις μολύνσεων μέσω του μηχανισμού «kill chain» και τεχνικών αποφυγής του εντοπισμού. Κατά το πρώτο εξάμηνο του 2016, η ESET παρατήρησε και πάλι μια σημαντική αύξηση στην ανίχνευση του Nymaim.

Επηρεάζοντας κυρίως την Πολωνία (54% των ανιχνεύσεων), τη Γερμανία (16%) και τις Ηνωμένες Πολιτείες (12%), η ανανεωμένη παραλλαγή ανιχνεύθηκε ως *Win32/TrojanDownloader.Nymaim.BA*, κάνοντας την επανεμφάνιση της ως μια ολοκληρωμένη εκστρατεία spearfishing με ένα κακόβουλο συνημμένο (Word .doc) που

περιέχει «παραπλανητικά» Marcos. Η προσέγγιση που χρησιμοποιείται για την παράκαμψη των προεπιλεγμένων ρυθμίσεων ασφαλείας του Microsoft Word μέσω μηχανισμών κοινωνικής μηχανικής, είναι αρκετά πειστική στις αγγλικές εκδόσεις του MS Word.

«Με προηγμένες τεχνικές αποφυγής του εντοπισμού, και δυνατότητες anti-VM, anti-debugging και control flow, αυτό το downloader που λειτουργεί σε δύο στάδια μεταφέροντας ransomware ως τελικό ωφέλιμο φορτίο, έχει πλέον εξελιχθεί και χρησιμοποιείται για να μεταφέρει spyware», λέει ο Cassius de Oliveira Puodzius, Security Researcher της ESET Latinoamerica.

Τον Απρίλιο, η συγκεκριμένη έκδοση ενώθηκε με υβριδική παραλλαγή του Nymaim και του *Gozi*, στοχεύοντας χρηματοπιστωτικά ιδρύματα στη Βόρεια Αμερική, ενώ εξαπλώθηκε και στη Λατινική Αμερική, κυρίως στη Βραζιλία. Αυτή η παραλλαγή έχει δώσει στους κυβερνοεγκληματίες τη δυνατότητα απομακρυσμένης πρόσβασης στους παραβιασμένους υπολογιστές, αντί να έχει τα συνήθη αποτελέσματα κρυπτογράφησης αρχείων ή κλειδώματος.

Λόγω των ομοιοτήτων μεταξύ των στόχων που βρίσκονται σε χώρες με υψηλά και χαμηλά ποσοστά ανίχνευσης, μπορούμε να είμαστε σχετικά σίγουροι ότι τα χρηματοπιστωτικά ιδρύματα παραμένουν στο επίκεντρο αυτής της εκστρατείας.

«Η πλήρης καταγραφή αυτής της απειλής είναι ακόμα σε εξέλιξη. Ωστόσο, εάν υποψιάζεστε ότι ο υπολογιστής ή το δίκτυό σας έχει παραβιαστεί, σας συνιστούμε να ελέγξετε κατά πόσο οι διευθύνσεις IP και URL, που βρίσκονται στο πλήρες άρθρο, δεν βρίσκονται στο firewall και στα στοιχεία σύνδεσης με το διακομιστή μεσολάβησης. Σε κάθε περίπτωση, μπορεί να εφαρμοστεί μια στρατηγική πρόληψης από την απειλή βάζοντας σε blacklist τις IP που έχουν έρθει σε επαφή με αυτό το malware στο firewall και τις διευθύνσεις URL στο proxy, εφόσον το δίκτυό σας υποστηρίζει αυτό το είδος φιλτραρίσματος», καταλήγει ο Puodzius.

Όλη η ανάλυση είναι διαθέσιμη στο ενημερωτικό blog της ESET, Welivesecurity.com.