Η ESET ανακαλύπτει νέο εξελιγμένο backdoor της ομάδας κυβερνοεγκληματιών Turla

Η ESET έδωσε σήμερα στη δημοσιότητα στοιχεία σχετικά με την ανακάλυψη ενός νέου, προηγμένου backdoor που χρησιμοποιείται από την περιβόητη ομάδα κυβερνοεγκληματιών Turla. Οι ερευνητές της ESET είναι οι πρώτοι που εντοπίζουν αυτό το πρόσφατο backdoor, γνωστό ως Gazer, το οποίο εξελίσσεται διαρκώς από το 2016, στοχεύοντας σε θεσμικά όργανα στην Ευρώπη.

Τυπικά χαρακτηριστικά της ομάδας Turla

Στοχεύοντας σε κυβερνήσεις στην Ευρώπη και πρεσβείες σε όλο τον κόσμο εδώ και πολλά χρόνια, η ομάδα κατασκοπείας Turla είναι γνωστή για τις επιθέσεις τύπου «watering hole» και τις εκστρατείες spearphishing που χρησιμοποιεί στα θύματά της.

Οι ερευνητές της ESET έχουν καταγράψει ότι το Gazer, το backdoor που πρόσφατα ανακαλύφθηκε, έχει μολύνει αρκετούς υπολογιστές σε όλο τον κόσμο, με ένα μεγάλο μέρος των επιθέσεων να έχει στοχεύσει τη νοτιοανατολική Ευρώπη.

«Οι τακτικές, οι τεχνικές και οι διαδικασίες που συναντήσαμε εδώ είναι όμοιες με αυτές που συνήθως βλέπουμε στη δράση της ομάδας Turla», δήλωσε ο Jean-Ian Boutin, Senior Malware Researcher στην ESET. «Αρχικά εγκαταστάθηκε ένα πρώτο

backdoor, δηλαδή το Skipper, πιθανά χρησιμοποιώντας τεχνικές spearphishing, και στη συνέχεια εμφανίστηκε το δεύτερο backdoor στο παραβιασμένο σύστημα, στη συγκεκριμένη περίπτωσή το Gazer.»

Ανιχνεύοντας ένα backdoor που χρησιμοποιεί τεχνικές αποφυγής εντοπισμού

Όπως και τα άλλα εργαλεία που χρησιμοποιεί η ομάδα Turla για να εγκαταστήσει τα δεύτερα backdoor, όπως τα Carbon και Kazuar, το Gazer λαμβάνει κρυπτογραφημένες εντολές από ένα C&C server, που μπορούν να εκτελεστούν είτε σε ήδη μολυσμένο μηχάνημα είτε σε άλλο μηχάνημα στο δίκτυο.

Οι δημιουργοί του Gazer κάνουν επίσης εκτεταμένη χρήση της δικής τους προσαρμοσμένης κρυπτογράφησης, χρησιμοποιώντας τη δική τους βιβλιοθήκη με αλγόριθμους 3DES ή RSA. Τα κλειδιά RSA που βρίσκονται ενσωματωμένα στα backdoor περιέχουν το δημόσιο κλειδί του διακομιστή ελέγχου του εισβολέα και ένα ιδιωτικό κλειδί.

Αυτά τα κλειδιά είναι μοναδικά για κάθε δείγμα και χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που στέλνονται/λαμβάνονται από/προς τον C&C server. Επιπλέον, η περιβόητη ομάδα Turla εμφανίστηκε να χρησιμοποιεί ένα εικονικό σύστημα αρχείων στο μητρώο των Windows για να αποφεύγει τα antivirus και να συνεχίζει να επιτίθεται στο σύστημα.

«Η ομάδα Turla κάνει τα πάντα για να αποφύγει τον εντοπισμό σε ένα σύστημα», συμπληρώνει ο Boutin. «Η ομάδα αρχικά σβήνει αρχεία από παραβιασμένα συστήματα και στη συνέχεια μετασχηματίζει τις συμβολοσειρές και χρησιμοποιώντας διάφορες εκδόσεις backdoor τροποποιεί τα κείμενα σε εφαρμογές με τυχαίο τρόπο.

Σε αυτήν την τελευταία περίπτωση, οι δημιουργοί του Gazer άλλαξαν το κείμενο και εισήγαγαν γραμμές από βιντεοπαιχνίδια όπως «Only single player is allowed». Η ανακάλυψη αυτού του

νέου και αχαρτογράφητου backdoor από την ομάδα ερευνητών της ESET σηματοδοτεί ένα σημαντικό βήμα προς τη σωστή κατεύθυνση για την αντιμετώπιση του αυξανόμενου προβλήματος της κυβερνο-κατασκοπείας στον σημερινό ψηφιακό κόσμο.»

Για περισσότερες τεχνικές λεπτομέρειες σχετικά με το νέο backdoor της ομάδας Turla επισκεφθείτε το σχετικό blogpost ή κατεβάστε ολόκληρο το white paper από το WeLiveSecurity.com.

Η ESET δημιουργεί ένα ασφαλές περιβάλλον για «Το Χαμόγελο του Παιδιού»

Η ESET Hellas Cyprus ανέλαβε για άλλη μία χρονιά να διασφαλίσει στον οργανισμό «Το Χαμόγελο του Παιδιού» τις κατάλληλες συνθήκες για την αποτελεσματική προστασία του από τους ψηφιακούς κινδύνους. Η εταιρία πρόσφερε 300 άδειες της βραβευμένης της λύσης ESET Endpoint Antivirus, που διακρίνεται για την ισχυρή ανίχνευση, την εξαιρετική σταθερότητα και τις χαμηλές απαιτήσεις συστήματος, ώστε να μπορεί ο οργανισμός να συνεχίζει με ασφάλεια το πολύτιμο έργο του.

«Το Χαμόγελο του Παιδιού» έχει σκοπό να προασπίζεται καθημερινά τα δικαιώματα των παιδιών και να προσφέρει ασφάλεια σε χιλιάδες παιδιά στην Ελλάδα που βρίσκονται σε κίνδυνο. Εμείς στην ESET, έχουμε σκοπό να προστατεύουμε τις συσκευές

και τις λειτουργίες του όλο το 24ωρο , κρατώντας τα δεδομένα και την πολύτιμη τεχνογνωσία του ασφαλή, ώστε «Το Χαμόγελο του Παιδιού» να συνεχίζει το πολύτιμο έργο του» δήλωσε ο κ. Νεόφυτος Νεοφύτου, Διευθύνων Σύμβουλος της ESET Middle East, Hellas & Cyprus.

Η λύση ESET Endpoint Antivirus αποτελεί μία από τις πιο αξιόπιστες επιλογές για ολοκληρωμένη και ισχυρή προστασία Endpoints. Διαθέτει ανώτερη τεχνολογία εντοπισμού και υποστήριξη virtualization, για να εξαλείφει όλων των ειδών τις απειλές, υποστηρίζοντας και εικονικές μηχανές. Απελευθερώνει περισσότερους πόρους συστήματος για κρίσιμα προγράμματα, από τα οποία οι χρήστες εξαρτώνται σε καθημερινή βάση, μπλοκάροντας παράλληλα μη εξουσιοδοτημένες συσκευές. Χάρη στην αναγνωρισμένη τεχνολογία ESET NOD32®, με τις λειτουργίες Exploit Blocker και Advanced Memory Scanner είναι σε θέση να εξουδετερώνει όλες τις εξελιγμένες απειλές, ενώ είναι πλήρως παραμετροποιήσιμη μέσω της νέας web-κονσόλας ESET Remote Administrator.

Computer Bild: Το ESET Internet Security είναι η

μοναδική λύση που προστατεύει από το Ransomware και το αφαιρεί

Η ESET σημείωσε ξανά σημαντικές επιδόσεις στις πρόσφατες δοκιμές «Internet Security Test» του γερμανικού Computer Bild, του κορυφαίου περιοδικού υπολογιστών στην Ευρώπη. Η λύση ESET Internet Security 2017 διακρίθηκε με το ασημένιο μετάλλιο ανάμεσα στα οκτώ προϊόντα που συμμετείχαν στις δοκιμές. Στο σχετικό αφιέρωμα, το Computer Bild τονίζει ιδιαίτερα την προστασία που προσφέρει η ESET ενάντια στο ransomware, λέγοντας ότι ήταν η «καλύτερη λύση σε επίπεδο ευκολίας στη χρήση» από όλες όσες συμμετείχαν στις δοκιμές.

«Απλή και καλή … Ο απρόσμενος περσινός νικητής αποδεικνύει φέτος ότι η νίκη του δεν είναι τυχαία», αναφέρει το Computer Bild. *«Η λύση της ESET ήταν η μόνη στις δοκιμές που όχι μόνο εξουδετέρωσε το επικίνδυνο ransomware, αλλά κατάφερε επίσης με επιτυχία να το αφαιρέσει από τους μολυσμένους υπολογιστές»* αναφέρεται στο αφιέρωμα του περιοδικού. Επιπλέον, η λύση της ESET ήταν η μία από τις δύο που δεν κατέγραψαν κανένα false positive στις δοκιμές.

«Σίγουρα δεν είναι σύμπτωση ότι η τεχνολογία μας αποσπά και πάλι υψηλή βαθμολογία στις καθιερωμένες δοκιμές του Computer Bild. Θα προτιμούσαμε να είχαμε λάβει το χρυσό μετάλλιο, όπως πέρυσι, αλλά και η δεύτερη θέση, με μία διαφορά μόλις 0,06 βαθμών, είναι εξίσου καλή» δήλωσε ο Stefan Thiel, Country Manager της ESET DACH (Γερμανία, Αυστρία και Ελβετία).

Πέρυσι, το ESET Smart Security 9 απέσπασε το βραβείο «Golden Computer» ως η καλύτερη λύση στην κατηγορία «ασφάλεια για οικιακούς χρήστες», αποτελώντας την κορυφαία επιλογή των αναγνωστών του Computer Bild. Και λίγους μήνες νωρίτερα, η ESET κέρδισε στις απαιτητικές δοκιμές του Computer Bild.

Παράλληλα, και ο διακεκριμένος γερμανικός οργανισμός Stiftung Warentest έδωσε εξαιρετικές βαθμολογίες στην λύση ESET Internet Security 2017. Κατατάσσοντας την στις τρεις πρώτες μεταξύ των 18 λύσεων που συμμετείχαν στις δοκιμές, επεσήμανε ιδιαίτερα την ύπαρξη πρόσθετων χαρακτηριστικών, καθώς και τη φιλικότητα στη χρήση.

Τέλος, το ESET Remote Administrator σημείωσε πολύ καλές επιδόσεις στις πρόσφατες δοκιμές του PC Magazin στη Γερμανία, και αναδείχθηκε νικητής κατά τη σύγκριση τιμής / απόδοσης.

Έρευνα της IDC για την ESET: Σύγχυση στις επιχειρήσεις σχετικά με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων της ΕΕ

Η ESET, ο κορυφαίος κατασκευαστής λογισμικού IT ασφάλειας με έδρα την Ε.Ε., συνεργάστηκε με την κορυφαία εταιρία αναλύσεων IDC, προκειμένου να διερευνήσει πως προσεγγίζουν μικρές και μεσαίες επιχειρήσεις σε επιλεγμένες χώρες τον Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) της Ε.Ε. και την ασφάλεια των endpoints. Τα αποτελέσματα δείχνουν ότι στις ευρωπαϊκές επιχειρήσεις εξακολουθεί να επικρατεί αβεβαιότητα

σχετικά με τον κανονισμό. Σχεδόν το 78% των ιθύνοντων σε θέματα IT σε περισσότερες από 700 ευρωπαϊκές εταιρίες είτε δεν κατανοούν πως θα τις επηρεάσει ο κανονισμός ή δεν τον γνωρίζουν καθόλου. Ωστόσο, πάνω από το ένα τρίτο των εταιριών επιθυμούν την κρυπτογράφηση, ένα θέμα που θίγεται από τον Κανονισμό Προστασίας Προσωπικών Δεδομένων. Αυτά και άλλα ευρήματα της έρευνας της IDC, που πραγματοποιήθηκε για λογαριασμό της ESET, αποκαλύπτονται στο Mobile World Congress στη Βαρκελώνη. Μέχρι τις 2 Μαρτίου 2017, οι ειδικοί της ESET θα παρουσιάζουν το συγκεκριμένο θέμα στο περίπτερο της ESET (Hall 5, booth B05).

«Το 63% των επιβεβαιωμένων data breaches αποδίδονται σε κλεμμένα ή «σπασμένα» passwords, γεγονός που αποδεικνύει τη σημασία ενός πρόσθετου ή εναλλακτικού παράγοντα πιστοποίησης της ταυτότητας … Η ανωνυμοποίηση των δεδομένων είναι η μία επιλογή, η κρυπτογράφηση είναι ή άλλη. Και οι δύο έχουν πλεονεκτήματα και μειονεκτήματα. Η ανωνυμοποίηση είναι καλή, αλλά δεν μπορεί να «επικρατήσει» στην περίπτωση συσχετισμού από περισσότερες πηγές. Η κρυπτογράφηση επιλύει αυτό το ζήτημα, αλλά – τουλάχιστον μέχρι πρόσφατα – θεωρείται υπερβολικά πολύπλοκη και ακριβή για τις περισσότερες μικρές και μεσαίες επιχειρήσεις», αναφέρει ο Mark Child, Research Manager της IDC, στην έκθεση. *«Η προστασία πελατών και συνεργατών είναι ζήτημα υψίστης σημασίας για να διασφαλιστεί η διαρκής επιτυχία και η επιβίωση οποιασδήποτε επιχειρηματικής οντότητας. Ωστόσο, οι εταιρίες πλέον αντιλαμβάνονται όλο και περισσότερο την επιχειρηματική αξία των δεδομένων τους και αναγνωρίζουν την επέκταση του κανονιστικού πλαισίου που πρέπει να σεβαστούν, καθώς και των κυρώσεων που επιβάλλονται σε περίπτωση μη συμμόρφωσης»* προσθέτει ο Child.

Παρόλα αυτά, η πρωτοποριακή νομοθεσία της Ε.Ε. δεν είναι πλήρως κατανοητή από τις επιχειρήσεις. Από τις εταιρίες που γνωρίζουν τον Κανονισμό Προστασίας Προσωπικών Δεδομένων, το 20% ισχυρίζεται ότι έχει ήδη συμμορφωθεί, το 59% αναφέρει ότι προσπαθεί να οδηγηθεί προς αυτή την κατεύθυνση, και το 21%

δηλώνει ότι δεν είναι καθόλου έτοιμο. Η IDC διεξήγαγε την έρευνα της μεταξύ επαγγελματιών του IT χώρου σε περισσότερες από 700 επιχειρήσεις στην Τσεχική Δημοκρατία, τη Γερμανία, την Ιταλία, τις Κάτω Χώρες, τη Σλοβακία, την Ισπανία και το Ηνωμένο Βασίλειο κατά τη διάρκεια του 4ου τριμήνου του 2016.

Ένα άλλο ενδιαφέρον εύρημα της IDC είναι το πώς προσεγγίζουν οι ευρωπαϊκές μικρές και μεσαίες επιχειρήσεις την κρυπτογράφηση. *«Πολλοί οργανισμοί αναγνωρίζουν ότι το υπάρχον λογισμικό antimalware που διαθέτουν είναι ανεπαρκές για το σημερινό περιβάλλον απειλών, και οι μισοί από τους ερωτηθέντες ανέφεραν αυτό ως το σημαντικότερο πεδίο για να προσθέσουν ή να αναβαθμίσουν»,* λέει ο Child της IDC. Η κρυπτογράφηση, η οποία αναφέρεται στον Κανονισμό Προστασίας Προσωπικών Δεδομένων, είναι ζητούμενο για το 36% των ερωτηθέντων.

«Η ESET είναι μία από τις εταιρίες που ασχολήθηκε με την κρυπτογράφηση νωρίς, με την λύση κρυπτογράφησης DESlock και προσφέρει εγγυήσεις στις επιχειρήσεις για να ανταποκριθούν στις απαιτήσεις της Ε.Ε.», λέει ο Pavol Balaj, Head of Business Development in EMEA της ESET, μιλώντας στο Mobile World Congress.

Για περισσότερες πληροφορίες σχετικά με τον Κανονισμό Προστασίας Προσωπικών Δεδομένων, και πώς η ESET βοηθά τις επιχειρήσεις να ετοιμαστούν για αυτόν, οι ενδιαφερόμενοι μπορούν να διαβάσουν το σχετικό whitepaper και να επισκεφθούν την ειδική σελίδα.

Περισσότερες πληροφορίες σχετικά με τα αποτελέσματα της έρευνας της IDC, καθώς και αντίγραφο όλου του whitepaper, διατίθενται στην ειδική ιστοσελίδα της ESET.

Η ESET στο Mobile World Congress: Πάνω από 50% αύξηση του Android Ransomware το 2016

Η ESET, ο κορυφαίος κατασκευαστής λογισμικού IT ασφάλειας με έδρα την Ε.Ε., κατέγραψε μια αύξηση πάνω από 50% στην ανίχνευση του Android ransomware το 2016, που αποτελεί ιστορικά το μεγαλύτερο αριθμό προσπαθειών για διείσδυση σε συσκευές. Η ESET παρουσιάζει τα τελευταία ετήσια δεδομένα που βασίζονται στην τεχνολογία LiveGrid® στο white paper *«Trends in Android Ransomware»*. Τα ευρήματα αποκαλύπτονται λίγο πριν το Mobile World Congress, που πραγματοποιείται στη Βαρκελώνη (27 Φεβρουαρίου – 2 Μαρτίου 2017).

«Συνολικά παρατηρήσαμε μια αύξηση στην ανίχνευση κακόβουλου λογισμικού σε συσκευές Android κατά περίπου 20%, με το ransomware σε αυτή την πλατφόρμα να αυξάνεται με ολοένα ταχύτερο ρυθμό. Παρόλο που η ESET κατέγραψε τη μεγαλύτερη αύξηση κατά το πρώτο εξάμηνο του 2016, δεν μπορούμε με καμία σιγουριά να πούμε ότι αυτή η απειλή θα εξαφανιστεί σύντομα», λέει ο Chief Technology Officer της ESET Juraj Malcho, ο οποίος θα ασχοληθεί με το συγκεκριμένο θέμα στο MWC 2017.

Οι δημιουργοί του crypto-ransomware, που κρυπτογραφεί αρχεία και κλειδώνει την οθόνη συσκευών, έχουν εξασκηθεί τους τελευταίους 12 μήνες στο να αντιγράφουν αποτελεσματικές

τεχνικές που χρησιμοποιούνται κατά τις επιθέσεις κακόβουλου λογισμικού σε desktop. Έχουν επίσης αναπτύξει τις δικές τους πιο εξελιγμένες μεθόδους ειδικά για στόχους σε Android συσκευές.

Εκτός από τις πιο διαδεδομένες τακτικές εκφοβισμού που χρησιμοποιεί το «police ransomware» που κλειδώνει οθόνες, οι εγκληματίες του κυβερνοχώρου προσπαθούν να διατηρούν ένα χαμηλό προφίλ, κρυπτογραφώντας το κακόβουλο φορτίο και «θάβοντάς» το ακόμη πιο βαθιά στις μολυσμένες εφαρμογές.

Το 2015, η ESET είχε παρατηρήσει ότι το ενδιαφέρον των δημιουργών του Android ransomware είχε μετατοπιστεί από τους χρήστες συσκευών στην Ανατολική Ευρώπη στους χρήστες στις ΗΠΑ. Ωστόσο, το περασμένο έτος εμφανίστηκε αυξανόμενο ενδιαφέρον στην ασιατική αγορά. *«Πράγματι, μπορούμε να πούμε ότι το ransomware που επιτίθεται σε Android έχει γίνει μια παγκόσμια απειλή μεγάλης κλίμακας»* προσθέτει ο Malcho.

Για πλήρη πρόσβαση στα ευρήματα, το white paper «Trends in Android Ransomware» είναι διαθέσιμο στο ειδησεογραφικό site της ESET WeLiveSecurity.com. Περισσότερες πληροφορίες σχετικά με το συγκεκριμένο θέμα κατά το Mobile World Congress, οι ενδιαφερόμενοι μπορούν να αντλήσουν από την ειδική σελίδα της ESET καθώς και να επισκεφθούν το περίπτερο της εταιρίας στο Συνέδριο στη Βαρκελώνη.

Ανακάλυψη της ESET: Νέο Downloader επιτίθεται σε Android «μασκαρεμένο» ως Update του Flash Player

Οι ερευνητές της ESET ανακάλυψαν μια νέα και επικίνδυνη εφαρμογή που στοχοποιεί συσκευές Android προχωρώντας σε λήψη και εγκατάσταση κακόβουλου λογισμικού. Το trojan, που εντοπίστηκε από το λογισμικό ασφαλείας της ESET ως Android / TrojanDownloader.Agent.JI, εξαπλώνεται μέσω παραβιασμένων ιστοσελίδων και εμφανίζεται ως μια ενημέρωση του Flash Player. Πρόκειται για μία από τις απειλές για Android που θα παρουσιαστούν από την ESET στο Mobile World Congress.

Αφού εγκατασταθεί, το κακόβουλο λογισμικό δημιουργεί στο Android μία ψεύτικη υπηρεσία για εξοικονόμηση ενέργειας της μπαταρίας παρακινώντας το θύμα να της δώσει πρόσβαση στις λειτουργίες του Android Accessibility. Αν ο χρήστης δώσει άδεια στις δυνατότητες «*Monitor your actions*», «*Retrieve window content*» και «*Turn on Explore by Touch*» ο εισβολέας μπορεί να μιμηθεί τις ενέργειες του χρήστη εμφανίζοντας στην οθόνη ό,τι θέλει.

« Σε περιπτώσεις που ερευνήσαμε, αυτό το trojan δημιουργήθηκε για να κατεβάσει ένα άλλο trojan που είχε σχεδιαστεί για να αποσπάσει χρήματα από τραπεζικούς λογαριασμούς. Ωστόσο, μόνο μια μικρή αλλαγή στον κώδικα θα σήμαινε μόλυνση του χρήστη με spyware ή ransomware» προειδοποιεί ο Lukáš Štefanko, Malware Researcher της ESET, επικεφαλής της ανάλυσης.

Η βασική ένδειξη ότι μια συσκευή έχει μολυνθεί με κακόβουλο λογισμικό αποτελεί η παρουσία της επιλογής «Saving Battery» μεταξύ των υπηρεσιών στο μενού Accessibility. Σε μια τέτοια περίπτωση, ο χρήστης πρέπει είτε να χρησιμοποιήσει μια

αξιόπιστη εφαρμογή ασφάλειας για κινητά, όπως το ESET Mobile Security & Antivirus για να αφαιρέσει την απειλή, είτε να απεγκαταστήσει την εφαρμογή πηγαίνοντας στο Ρυθμίσεις -> Διαχείριση εφαρμογών -> Flash-Player.

Σε περίπτωση που ο χρήστης έχει εξαπατηθεί παραχωρώντας στην εφαρμογή δικαιώματα διαχείρισης της συσκευής, είναι απαραίτητο να απενεργοποιήσει καταρχήν τα δικαιώματα διαχειριστή, μεταβαίνοντας στις Ρυθμίσεις -> Ασφάλεια -> Flash-Player.

«*Δυστυχώς, η απεγκατάσταση του downloader δεν αφαιρεί τις κακόβουλες εφαρμογές που πιθανά έχει ήδη εγκαταστήσει. Όπως ισχύει και για το downloader, ο καλύτερος τρόπος για τον καθαρισμό της συσκευής είναι να χρησιμοποιηθεί μία λύση ασφάλειας για κινητά*» συνιστά ο Lukáš Štefanko.

Οι ειδικοί της ESET έχουν ετοιμάσει μια σειρά από βασικές συμβουλές για την πρόληψη της μόλυνσης από κακόβουλο λογισμικό που επιτίθεται σε κινητά:

– Κατεβάστε εφαρμογές ή ενημερώσεις μόνο από αξιόπιστη πηγή – στην περίπτωση του update του Adobe Flash Player, το μόνο ασφαλές μέρος είναι το επίσημο site της Adobe. Να ελέγχετε πάντα τη διεύθυνση URL στο πρόγραμμα περιήγησής σας

– Δώστε προσοχή στην πρόσβαση και τα δικαιώματα που ζητούν να αποκτήσουν οι εφαρμογές σας.

– Χρησιμοποιήστε μια αξιόπιστη λύση Mobile Security.

Οι ενδιαφερόμενοι μπορούν να βρουν περισσότερες πληροφορίες σχετικά με το επικίνδυνο downloader ή για την προληπτική τεχνολογία της ESET. Οι ειδικοί της ESET θα βρίσκονται στο φετινό Mobile World Congress προσφέροντάς πληροφορίες για την ασφάλεια των κινητών.

Η ESET εστιάζει στο κρίσιμο θέμα του Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR) της ΕΕ

Τη στρατηγική της σχετικά με τον Ευρωπαϊκό Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR) θα παρουσιάσει η ESET στο Mobile World Congress που θα διεξαχθεί στη Βαρκελώνη, στις 27 Φεβρουαρίου – 2 Μαρτίου του 2017. Ο κανονισμός θα τεθεί σε ισχύ σε ένα χρόνο από σήμερα, με σημαντικές συνέπειες για τις επιχειρήσεις σε όλη την Ευρώπη. Πρέπει να τονιστεί ότι ο πρωταρχικός στόχος του GDPR είναι να διασφαλιστεί η προστασία της ιδιωτικής ζωής των πολιτών της ΕΕ. Σε αυτό το πλαίσιο, η ESET θα παρουσιάσει ένα white paper σχετικά με τις επικείμενες νομικές απαιτήσεις, που θα ισχύουν από τον Μάιο του 2018, με αναλυτικές πληροφορίες για το πώς οι λύσεις ασφάλειας της ESET ανταποκρίνονται πλήρως στις ρυθμίσεις του κανονισμού.

Από το επόμενο έτος, μία εταιρία οφείλει να συμμορφωθεί με τον κανονισμό GDPR , εφόσον δραστηριοποιείται: «στην παροχή δωρεάν ή επί πληρωμή αγαθών ή υπηρεσιών, που περιλαμβάνουν διαχείριση προσωπικών δεδομένων σε άτομα εντός της ΕΕ, και στην παρακολούθηση της συμπεριφοράς των ατόμων από όπου προκύπτουν τα προσωπικά δεδομένα εντός της ΕΕ» αναφέρει η ESET στο white paper, για τη δημιουργία της οποίας επιστρατεύτηκε η εμπειρία

και η κατάρτιση της νομικής εταιρίας Kemp Jones Solicitors LLP. Αναφέρεται επίσης ότι «παρά την εισαγωγή ενός βελτιωμένου νομικού πλαισίου, ο κανονισμός GDPR είναι ακόμα πιθανό να επιφέρει σημαντικές αλλαγές σε πολλές επιχειρήσεις, απαιτώντας σημαντικό χρόνο προσαρμογής».

«Ο κανονισμός GDPR δεν εστιάζει μόνο σε εταιρείες που εδρεύουν στην ΕΕ. Αυτές οι αλλαγές θα επηρεάσουν κάθε επιχείρηση που επεξεργάζεται προσωπικά δεδομένα πολιτών της ΕΕ. Η ESET προσφέρει λύσεις που θα βοηθήσουν τις επιχειρήσεις στην εκπλήρωση των απαιτήσεων του κανονισμού και ταυτόχρονα στην προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ», συμπληρώνει ο Pavol Balaj, ESET Head of Business Development in EMEA, που θα παρευρίσκεται στο Συνέδριο MWC.

Ο κανονισμός GDPR καθορίζει επίσης τα μέτρα που κρίνονται κατάλληλα, δίνοντας έμφαση στην κρυπτογράφηση των δεδομένων. Σε γενικές γραμμές, τα κύρια οφέλη της τεχνολογίας κρυπτογράφησης είναι η δύναμή της – χάρη στους ισχυρούς αλγόριθμους και των ολοένα και αυξανόμενων σε μέγεθος κλειδιών (bits) – η ευρεία διαθεσιμότητά και το σχετικά χαμηλό κόστος εφαρμογής, που την καθιστούν αποδεκτή ακόμη και από ορισμένες εθνικές αρχές.

«Η τεχνολογία κρυπτογράφησης DESlock από την ESET, προσφέρει περισσότερα από τα βασικά. Παρέχει στους εταιρικούς πελάτες μια λύση εύκολη στην εγκατάσταση και στη χρήση ακόμα και για χρήστες που δεν διαθέτουν τεχνική κατάρτιση, επιτρέποντας την απομακρυσμένη διαχείριση των κλειδιών κρυπτογράφησης, των ρυθμίσεων και των πολιτικών ασφαλείας. Επιπλέον, επιτρέπει στους χρήστες να κρυπτογραφήσουν με ασφάλεια σκληρούς δίσκους, αφαιρούμενα μέσα, αρχεία και e-mail», αναφέρεται στο white paper της ESET.

Για περισσότερες πληροφορίες σχετικά με τον κανονισμό GDPR, καθώς και το πώς η ESET φροντίζει να προετοιμάσει τις επιχειρήσεις αναφορικά με τις νέες ρυθμίσεις του, οι ενδιαφερόμενοι μπορούν να διαβάσουν το σχετικό «White Paper»

και να επισκεφθούν την ειδική σελίδα της ESET σχετικά με την κρυπτογράφηση.

Η ESET παρουσιάζει το Threat Intelligence, την Κρυπτογράφηση Ransomware και την Προστασία Προσωπικών Δεδομένων στο Mobile World Congress 2017

Η ESET συμμετέχει στο Mobile World Congress στη Βαρκελώνη (27 Φεβρουαρίου – 2 Μαρτίου 2017), όπου θα παρουσιάσει τις πρόσφατες λύσεις της ειδικά για πλατφόρμες business και mobile, την τελευταία της έρευνα καθώς και τη στρατηγική που θα ακολουθήσει σύμφωνα με τον κανονισμό προστασίας προσωπικών δεδομένων της ΕΕ. Περισσότερες πληροφορίες σχετικά με την παρουσία της εταιρίας στο συνέδριο είναι διαθέσιμα στην ειδική σελίδα.

Στο συνέδριο θα παρουσιαστούν οι νέες υπηρεσίες Threat Intelligence της ESET. Οι υπηρεσίες προβλέπουν και προειδοποιούν τις επιχειρήσεις για κινδύνους που τις απειλούν σε πραγματικό χρόνο, προσφέροντας τους ακόμη μεγαλύτερη

ευελιξία για να προσαρμόζονται σε ένα ταχύτατα μεταβαλλόμενο τοπίο απειλών. Στοχευμένες επιθέσεις, προηγμένες επιθέσεις APTs, zerodays και botnet, συμπεριλαμβάνονται στην ανάλυση των υπηρεσιών Threat Intelligence. Επιπλέον, οι υπηρεσίες είναι διαθέσιμες σε ομάδες ασφάλειας μεγάλων οργανισμών και επιχειρησιακών κέντρων ασφάλειας (Security Operation Centers) για την ανάλυση συγκεκριμένων ειδών κακόβουλου λογισμικού και την παροχή εξειδικευμένων πληροφοριών σχετικά με τη λειτουργία και τις επιπτώσεις τους.

Στην τελευταία έρευνα της ESET, σημαντική θέση κατέχει το θέμα των απειλών σε κινητές συσκευές και, συγκεκριμένα, το ransomware που επιτίθεται στην πλατφόρμα Android κρυπτογραφώντας αρχεία και κλειδώνοντας την οθόνη. Οι ερευνητές της ESET θα παρουσιάσουν ένα white paper με τα τελευταία στοιχεία, ενώ ο Chief Technology Officer της ESET, Juraj Malcho, θα πραγματοποιήσει παρουσίαση σχετικά με το συγκεκριμένο θέμα στο συνέδριο. Σε σχετική του δήλωση ανέφερε «Κάθε χρόνο παρατηρούμε τη σταδιακή αύξηση της απειλής αυτής, γενικά σε όλες τις πλατφόρμες και πιο συγκεκριμένα στις κινητές συσκευές. Παρόλα αυτά, οι χρήστες ακόμη δεν προστατεύουν τον εαυτό τους σωστά, ούτε αφιερώνουν την πρέπουσα προσοχή στην υπεύθυνη online συμπεριφορά».

Οι ενδιαφερόμενοι μπορούν να διαβάσουν περισσότερα για τα αποτελέσματα της έρευνας στα σχετικά blogposts «Android ransomware spreads further, with new methods in its toolbox», «Security by design for mobile device manufacturers» και «Indirect damage: Why service providers should care about customer security» στο ειδησεογραφικό portal WeLiveSecurity.com της ESET.

Ένα άλλο βασικό σημείο όπου θα εστιάσει η ESET στη Βαρκελώνη θα είναι ο ευρωπαϊκός κανονισμός προστασίας προσωπικών δεδομένων. Θα παρουσιαστούν ευρήματα από μια έρευνα που πραγματοποιήθηκε από την IDC για λογαριασμό της σε ESET σε ιθύνοντες του χώρου της πληροφορικής από διάφορες ευρωπαϊκές χώρες αναφορικά με την προστασία των δεδομένων και τον

Ευρωπαϊκό Κανονισμό Γενικής Προστασίας Δεδομένων (GDPR).

«Η ασφάλεια των δεδομένων είναι ένα βασικό στοιχείο του κανονισμού της ΕΕ που υποχρεώνει τις επιχειρήσεις να μεριμνούν για την επαρκή προστασία των προσωπικών δεδομένων. Οι λύσεις και η τεχνολογία της ESET είναι κατάλληλα προετοιμασμένες για να αντιμετωπίσουν τις κύριες πτυχές των απαιτήσεων αυτών της ΕΕ», αναφέρει ο Palo Balaj, Head of EMEA Business Development της ESET, ο οποίος θα βρίσκεται επίσης στο περίπτερο της ESET στο συνέδριο.

Μεταξύ άλλων κορυφαίων στελεχών της ESET, ο Ignacio Sbampato, Chief Business Officer, και ο Miroslav Mikus, EMEA Sales and Marketing Director, θα είναι διαθέσιμοι για συναντήσεις.

Για τους συμμετέχοντες από το χώρο των επιχειρήσεων, ο Juraj Malcho, CTO της ESET θα παρουσιάσει τις τελευταίες τάσεις στο χώρο της ασφάλειας στο ειδικά σχεδιασμένο Networking Event της ESET την Τρίτη 28 Φεβρουαρίου, ώρες 16.00-18.00, στο MWC Networking Garden 3/5.

Οι προβλέψεις της ESET για τη νέα χρονιά στην έκθεση

«Trends 2017: Security held ransom»

Σε μία προσπάθεια να βοηθήσει επιχειρήσεις και οικιακούς χρήστες να προστατευτούν καλύτερα κατά το 2017, η ESET ζήτησε από τους ειδικούς της να ετοιμάσουν μία έκθεση με τις κυριότερες τάσεις σε ζητήματα ασφάλειας. Στην έκθεση «*Trends 2017: Security held ransom*» περιλαμβάνονται πληροφορίες σχετικά με τις πιο πρόσφατες επιθέσεις, καθώς και προβλέψεις για τα θέματα που θα απειλήσουν την ασφάλεια στον κυβερνοχώρο κατά το τρέχον έτος. Η έκθεση διατίθεται δωρεάν στους αναγνώστες, προσφέροντας τους τη δυνατότητα να ενημερωθούν και να είναι καλύτερα προετοιμασμένοι για την αντιμετώπιση των σχετικών προκλήσεων.

Με βάση τις πληροφορίες που συγκεντρώθηκαν από τα Εργαστήρια Ερευνών της ESET σε όλο τον κόσμο, η έκθεση δείχνει ότι και το 2017 θα αποτελέσει «χρονιά ransomware». Όπως αναφέρεται στην έκθεση: «*Μία νέα τάση διαφαίνεται στον ορίζοντα: Το Ransomware of Things ή RoT, δηλαδή η δυνατότητα των εγκληματιών του κυβερνοχώρου να επιτίθενται σε συσκευές κρατώντας τις «όμηρους» και, στη συνέχεια, να απαιτούν την καταβολή λύτρων με αντάλλαγμα την αποκατάσταση του ελέγχου από το χρήστη*».

Με το κόστος της εγκληματικότητας στον κυβερνοχώρο να έχει αυξηθεί περισσότερο από 200% κατά την τελευταία πενταετία, η ESET θέλησε με την έκθεση αυτή όχι μόνο να βοηθήσει τις επιχειρήσεις και τους χρήστες να κατανοήσουν τις προηγμένες τακτικές και τεχνικές που χρησιμοποιούνται από τους χάκερ, αλλά και να συντελέσει στην προστασία τους από τις απειλές κατά το 2017. Είναι σημαντικό όλοι οι χρήστες να έχουν επίγνωση από τι είδους επιθέσεις κινδυνεύουν, καθώς το έγκλημα στον κυβερνοχώρο έχει σημαντικές επιπτώσεις: επηρεάζει τους οικονομικούς πόρους που διαθέτουν χρηστες και οργανισμοί για να προστατευτούν, και επιδρά στη φήμη, πλήττωντας την σε περίπτωση που πέσουν θύματα επίθεσης. Η έκθεση υπογραμμίζει

επίσης τη σημασία της συνεχούς εκπαίδευσης ως μία από τις βασικές προϋποθέσεις για να παραμείνει κανείς ασφαλής όσο βρίσκεται online και παρουσιάζει απλά βήματα για την αύξηση του γνωστικού επιπέδου στους αναγνώστες.

Η έκθεση «The *Trends 2017: Security held ransom* report», χωρίζεται σε εννέα κεφάλαια, το καθένα με επίκεντρο μια σημαντική πτυχή της ασφάλειας των πληροφοριών. Τα περισσότερα από τα κεφάλαια ασχολούνται με τις απειλές, είτε βάσει τύπου (Ransomware, Ευπάθειες, και Mobile) είτε βάσει κλάδου (Υγεία, Υποδομές Ζωτικής Σημασίας, και Gaming). Φιλοξενείται επίσης η θέση της ESET για τις ευρύτερες εξελίξεις στον κλάδο της ασφάλειας, που προβλέπεται να διαδραματίσουν ένα σημαντικότερο ρόλο το 2017.

Οι ενδιαφερόμενοι μπορούν να κατεβάσουν ολόκληρη την έκθεση εδώ: ESET Trends 2017: Security held ransom report ή να διαβάσουν μία πιο σύντομη εκδοχή της στο WeLiveSecurity.com, καθώς επίσης να αποκτήσουν http://www.welivesecurity.com/περισσότερες πληροφορίες σχετικά με τις προηγμένες τεχνολογίες ασφάλειας της ESET και να ενημερωθούν για όλα τα νεότερα για την ασφάλεια του κυβερνοχώρου.

Η ESET εκδίδει ετήσια έκθεση με τις ευπάθειες που παρουσιάστηκαν στα Microsoft Windows

Την ετήσια έκθεση «Windows Exploitation in 2016» εξέδωσε η ESET, στην οποία συνοψίζονται τα «θετικά και αρνητικά» που παρουσιάστηκαν στο πιο ευρέως χρησιμοποιούμενο λειτουργικό σύστημα, τα Microsoft Windows®. Στις 25 σελίδες της έκθεσης, η ESET αναλύει τις ευπάθειες που εμφανίστηκαν κατά τη διάρκεια των τελευταίων 12 μηνών, παρέχοντας λεπτομέρειες σχετικά με τα πιο ευάλωτα επιμέρους στοιχεία, όπως τον Internet Explorer και τα User-Mode Components των Windows.

Συγκριτικά με τα περσινά στοιχεία, η φετινή έκθεση «Windows Exploitation in 2016» αποκαλύπτει ότι ο αριθμός των ευπαθειών που επιδιορθώθηκαν αυξήθηκε σε όλους τους τομείς, εκτός από ένα, τον Internet Explorer (IE), όπου παρουσιάστηκε μια απότομη μείωση του αριθμού των ευπαθειών από 242 σε 109, κατά τους τελευταίους δώδεκα μήνες.

Από την άλλη πλευρά, τα User-Mode Components των Windows, μια λειτουργία του επεξεργαστή, κατά την οποία τρέχουν οι περισσότερες εφαρμογές και κάποιοι οδηγοί για Windows OS, παρέμειναν το ίδιο δημοφιλή στους εγκληματίες του κυβερνοχώρου. Στην έκθεση, η ESET τοποθετεί τα User-Mode Components των Windows, με 116 ευπάθειες που επιδιορθώθηκαν, στην κορυφή του διαγράμματος για το 2016. Μεταξύ των πιο διαδεδομένων τρόπων που οι κυβερνοεγκληματίες κάνουν κατάχρηση των 0-days σε User-mode είναι η απομακρυσμένη εκτέλεση κώδικα και οι επιθέσεις «elevation of privileges». Παρότι εμφανίζεται πρώτη φορά στην έκθεση, το Microsoft Edge, έχει αποδειχτεί ανθεκτικό στην εκμετάλλευση, και πολύ κοντά στη δεύτερη θέση, του έχουν αποδοθεί οι πρώτες 111 «patched» ευπάθειες. Σε

αντίθεση με τον IE, το Edge διατηρεί σύγχρονα χαρακτηριστικά ασφαλείας, όπως το AppContainer ή διαδικασίες 64-bit για καρτέλες ενεργοποιημένες από προεπιλογή, τα οποία το καθιστούν λιγότερο ευάλωτο.

Η έκθεση «Windows Exploitation Report 2016» περιέχει αναλυτικά στατιστικά σχετικά με τις ευπάθειες που επιδιορθώθηκαν σε εκδόσεις των Windows που υποστηρίζονται από τη Microsoft, τα επιμέρους στοιχεία, τα προγράμματα περιήγησης στο Web, καθώς και τη σουίτα Office, και παρέχει επίσης πληροφορίες σχετικά με ενημερώσεις που έχουν εκδοθεί. Ο συγγραφέας της έκθεσης ρίχνει επίσης μια λεπτομερή ματιά στις τεχνικές μείωσης κινδύνου στις πιο πρόσφατες εκδόσεις των Windows και την αποτελεσματικότητα της ασφάλειας σε βασικά προγράμματα περιήγησης στο Web, καθώς αποτελούν πολύ ελκυστικούς στόχους για τους κυβερνοεγκληματίες.

Οι ενδιαφερόμενοι μπορούν να κατεβάσουν ολόκληρη την έκθεση Windows Exploitation in 2016 εδώ. Επιπλέον στοιχεία σχετικά με την ασφάλεια στο επίσημο blog της ESET, WeLiveSecurity.com, καθώς και περισσότερες πληροφορίες για τις προηγμένες τεχνολογίες ασφάλειας της ESET.