Kaspersky:Το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών στην Ευρώπη θεωρούν ότι οι παραβιάσεις είναι αναπόφευκτες

Το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών στην Ευρώπη θεωρούν ότι οι παραβιάσεις είναι αναπόφευκτες, αλλά πάρα πολλοί είναι «κολλημένοι» σε έναν φαύλο κύκλο κινδύνου

Οι υπεύθυνοι του τομέα της πληροφορικής στις επιχειρήσεις παγκοσμίως έχουν βρεθεί σε αδιέξοδο αναφορικά με την καταπολέμηση του ψηφιακού εγκλήματος. Δεν έχουν επιρροή στα ανώτερα ηγετικά στελέχη και δυσκολεύονται να δικαιολογήσουν τους προϋπολογισμούς που χρειάζονται, καθιστώντας, αναπόφευκτα, τις επιχειρήσεις στις οποίες εργάζονται πιο ευάλωτες. Το φαινόμενο αυτό είναι ένα από τα ευρήματα μιας νέας έκθεσης της Kaspersky Lab, η οποία διαπίστωσε ότι το 80% των Υπεύθυνων Ασφάλειας Πληροφοριών (CISOs) στην Ευρώπη θεωρούν ότι οι παραβιάσεις της ψηφιακής ασφάλειας είναι αναπόφευκτες, ενώ κατά κύριο λόγο ανησυχούν για τις ομάδες εγκληματιών με οικονομικό κίνητρο.

Από το cloud στους κακόβουλους εισβολείς: η επιφάνεια επιθέσεων διευρύνεται στις σύγχρονες επιχειρήσεις

Η άνοδος των ψηφιακών απειλών, σε συνδυασμό με τον ψηφιακό μετασχηματισμό που πολλές εταιρείες πραγματοποιούν επί του

παρόντος, καθιστά τον ρόλο του CISO όλο και πιο σημαντικό στη σύγχρονη επιχείρηση. Η Kaspersky Lab αναφέρει ότι η πίεση που δέχονται οι CISOs είναι τώρα μεγαλύτερη από ποτέ: το 57% θεωρεί ότι οι πολύπλοκες υποδομές που περιλαμβάνουν το cloud και η φορητότητα αποτελούν κορυφαία πρόκληση και το 50% ανησυχεί για τη συνεχιζόμενη αύξηση των ψηφιακών επιθέσεων.

Οι CISOs πιστεύουν ότι οι εγκληματικές συμμορίες με οικονομικό κίνητρο (40%) και οι κακόβουλες επιθέσεις (29%) είναι οι μεγαλύτεροι κίνδυνοι για τις επιχειρήσεις τους και αυτές είναι οι απειλές που είναι εξαιρετικά δύσκολο να αποφευχθούν: είτε επειδή εκκινούνται από «επαγγελματίες» είτε επειδή υποβοηθούνται από υπαλλήλους.

Οι προκλήσεις αιτιολόγησης του προϋπολογισμού αφήνουν τους CISOs να ανταγωνίζονται με άλλα τμήματα της εταιρείας

Οι προϋπολογισμοί που διατίθενται για την ψηφιακή ασφάλεια αναφέρθηκε ότι αυξάνονται. Περίπου οι μισοί (49%) CISOs αναμένουν ότι οι προϋπολογισμοί τους θα αυξηθούν στο μέλλον και το 49% των ερωτηθέντων αναμένει ότι οι προϋπολογισμοί θα παραμείνουν οι ίδιοι.

Ωστόσο, οι CISOs αντιμετωπίζουν σημαντικές προκλήσεις με τον προϋπολογισμό, επειδή είναι σχεδόν αδύνατο για αυτούς να προσφέρουν σαφή απόδοση επένδυσης (ROI) ή 100% προστασία ενάντια στις ψηφιακές επιθέσεις.

Για παράδειγμα, το 36% των CISOs δηλώνουν ότι δεν μπορούν να εξασφαλίσουν τους προϋπολογισμούς για την ασφάλεια στον τομέα της πληροφορικής, επειδή δεν μπορούν να εγγυηθούν ότι θα υπάρξει παραβίαση. Και όταν οι προϋπολογισμοί ασφάλειας θεωρούνται από μια επιχείρηση, ως μέρος των συνολικών δαπανών πληροφορικής, οι CISOs βρίσκονται αντιμέτωποι με άλλα τμήματα προκειμένου να εξασφαλίσουν τον απαραίτητο προϋπολογισμό. Ο δεύτερος πιο πιθανός λόγος για να μην λάβουν τον απαραίτητο προϋπολογισμό είναι ότι η ασφάλεια είναι μερικές φορές μέρος των συνολικών δαπανών πληροφορικής. Επιπλέον, ένας στους τρεις

CISOs (33%) δήλωσε ότι ο προϋπολογισμός θα μπορούσε να διατεθεί για ψηφιακά, cloud ή άλλα έργα πληροφορικής αντ' αυτού – τα οποία μπορεί να είναι σε θέση να αποδείξουν μια σαφέστερη ROI.

Οι CISOs χρειάζονται κοινό σε επίπεδο διοικητικού συμβουλίου, καθώς ο ψηφιακός μετασχηματισμός θα τεθεί σε ισχύ

Οι ψηφιακές επιθέσεις μπορούν να έχουν δραστικές συνέπειες για τις επιχειρήσεις: περισσότεροι από ένας στους τρεις ερωτηθέντες στην έρευνα της Kaspersky Lab αναγνώρισε τις ζημιές στη φήμη (28%) και τις οικονομικές (25%) ως τις πιο κρίσιμες συνέπειες μιας ψηφιακής επίθεσης.

Ωστόσο, παρά τον αρνητικό αντίκτυπο μιας ψηφιακής επίθεσης, μόνο το 26% των υπεύθυνων ασφάλειας του τομέα της πληροφορικής που συμμετείχαν στην έρευνα είναι μέλη του διοικητικού συμβουλίου στις αντίστοιχες επιχειρήσεις. Από εκείνους που δεν είναι μέλη του διοικητικού συμβουλίου, ένας στους τέσσερις (25%) πιστεύει ότι θα έπρεπε να είναι.

Η πλειονότητα των υπευθύνων της ασφάλειας πληροφορικής (58%) πιστεύει ότι εμπλέκονται επαρκώς στη λήψη επιχειρηματικών αποφάσεων τη δεδομένη στιγμή. Ωστόσο, καθώς ο ψηφιακός μετασχηματισμός καθίσταται καθοριστικός για τη στρατηγική κατεύθυνση των μεγάλων επιχειρήσεων, το ίδιο θα πρέπει να ισχύει και για την ψηφιακή ασφάλεια. Ο ρόλος του CISO πρέπει να αναπτυχθεί ώστε να αντικατοπτρίζει αυτές τις αλλαγές, δίνοντάς τους τη δυνατότητα να επηρεάζουν τις αποφάσεις.

Ο Maxim Frolov, VP Global Sales, στην Kaspersky Lab, δήλωσε: «*Ιστορικά, οι προϋπολογισμοί για την ψηφιακή ασφάλεια θεωρήθηκαν ως δαπάνες χαμηλής προτεραιότητας, αλλά αυτό δεν ισχύει πλέον. Η επιφάνεια των επιθέσεων ενάντια στις σύγχρονες επιχειρήσεις αυξάνεται, όπως και η συχνότητα και ο αντίκτυπος των ψηφιακών επιθέσεων και το κόστος των περιστατικών στον κυβερνοχώρο. Το αποτέλεσμα είναι ότι όλο και περισσότερα ανώτατα στελέχη αντιμετωπίζουν πλέον την ασφάλεια πληροφορικής*

ως επένδυση».

Και συνέχισε: «*Σήμερα, οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο βρίσκονται στην κορυφή της ατζέντας των Διευθύνοντων Συμβούλων, των CFOs και των Risk Officers. Στην πραγματικότητα, ο προϋπολογισμός για τον κυβερνοχώρο δεν είναι απλώς ένας τρόπος πρόληψης των παραβιάσεων και των καταστροφικών κινδύνων που συνδέονται με αυτούς – είναι ένας τρόπος για να προστατεύσουμε τη συνέχεια της επιχείρησης, καθώς και τις βασικές επενδύσεις μιας εταιρείας*».

Εδώ μπορείτε να βρείτε την πλήρη έκθεση.

Μπέρδεμα στο cloud: Δύο στις τρεις μικρομεσαίες επιχειρήσεις «παλεύουν» με τις υπερ-πολύπλοκες υποδομές πληροφορικής

Καθώς αναπτύσσονται οι επιχειρήσεις τους, οι εταιρείες υιοθετούν ολοένα και περισσότερο νέα επιχειρηματικά εργαλεία και υπηρεσίες cloud σε μια προσπάθεια να καταστήσουν την επαγγελματική ζωή των εργαζομένων πιο αποτελεσματική και ευέλικτη, καθώς και να μειώσουν τις δαπάνες. Σύμφωνα με την τελευταία έρευνα της Kaspersky Lab, σχεδόν τα δύο τρίτα (63%)

των εταιρειών που απασχολούν έως και 249 άτομα χρησιμοποιούν μια ή περισσότερες επιχειρηματικές εφαρμογές ως υπηρεσία (as-a-service). Ωστόσο, αυτή η τάση μεταξύ αναπτυσσόμενων εταιρειών για τη χρήση υπηρεσιών cloud για τη βελτιστοποίηση των λειτουργιών τους μπορεί επίσης να έχει αρνητικές επιπτώσεις, όπως απώλεια ελέγχου της ασφάλειας εφαρμογών και πολύτιμων δεδομένων πελατών.

Οι μικρομεσαίες επιχειρήσεις διευκολύνουν την ανάπτυξη με πλατφόρμες cloud

Τόσο οι μικρότερες εταιρείες όσο και εκείνες που διέρχονται από μια φάση ταχείας ανάπτυξης, βλέπουν τις τεχνολογίες cloud ως μια ευκαιρία για να διαχειριστούν τα επιχειρηματικά τους καθήκοντα με πιο αποτελεσματικό και οικονομικό τρόπο. Το 50% των εταιρειών με έως και 49 εργαζόμενους (πολύ μικρές επιχειρήσεις) και το 40% των εταιρειών με 50-249 εργαζόμενους (μικρομεσαίες επιχειρήσεις) έχουν προσωπικό που εργάζεται τακτικά εκτός γραφείου και χρειάζεται πρόσβαση σε δεδομένα και εφαρμογές μέσω του cloud. Και καθώς οι εταιρείες γίνονται μεγαλύτερες, αντιμετωπίζουν μια αυξανόμενη ανάγκη για υπηρεσίες cloud: το 73% των μικρομεσαίων επιχειρήσεων και το 56% των πολύ μικρών επιχειρήσεων χρησιμοποιούν τουλάχιστον μία υπηρεσία cloud. Μεταξύ των πιο δημοφιλών εργαλείων SaaS είναι οι υπηρεσίες email, αποθήκευσης εγγράφων και συνεργασίας, η χρηματοδότηση και η λογιστική.

IT, ψηφιακή ασφάλεια και έλλειψη ελέγχου

Ωστόσο, μια ενεργή χρήση των clouds μπορεί να έχει και κάποιες αρνητικές επιπτώσεις: οι υποδομές Πληροφορικής στους οργανισμούς ενοποιούν όλο και περισσότερες υπηρεσίες και εφαρμογές, αλλά μερικές φορές δεν φροντίζουν επαρκώς για την παροχή των απαιτούμενων επιπέδων ελέγχου και ορατότητας. Κατά συνέπεια, το 66% των εταιρειών με 1-249 εργαζομένους αντιμετωπίζουν δυσκολίες όσον αφορά στη διαχείριση αυτών των ετερογενών υποδομών Πληροφορικής.

Αυτή η αυξανόμενη πολυπλοκότητα απαιτεί από τις μικρομεσαίες επιχειρήσεις να υιοθετήσουν μια νέα προσέγγιση στη διαχείριση της υποδομής. Το πρόβλημα, ωστόσο, είναι ότι οι ειδικοί του τομέα της Πληροφορικής δεν διαθέτουν πάντοτε επαρκή εμπειρία για να αντιμετωπίσουν αυτήν την πρόκληση. Επιπλέον, το 14% των εταιρειών με 50-249 εργαζόμενους εμπιστεύονται τη διαχείριση της ασφάλειας του τομέα της Πληροφορικής σε μέλη του προσωπικού που δεν είναι απολύτως ειδικοί. Αυτό μπορεί να έχει ως αποτέλεσμα την εμφάνιση πραγματικών κινδύνων για την ψηφιακή ασφάλεια των εταιρειών που μπορεί να μην είναι πάντοτε σε θέση ή να μην έχουν χρόνο να αξιολογήσουν, καθώς εστιάζουν περισσότερο την προσοχή τους στην ανάπτυξη των επιχειρήσεων τους.

Ποιοι είναι υπεύθυνοι για την προστασία δεδομένων στις εφαρμογές που χρησιμοποιούνται as-a-service;

Ακόμη και στο πλαίσιο των λειτουργιών ασφάλειας πληροφοριών που αποδεικνύονται δευτερεύουσες στην ανάπτυξη των επιχειρήσεων, οι μικρομεσαίες επιχειρήσεις εξακολουθούν να συνειδητοποιούν πόσο σημαντικό είναι για αυτές να εξασφαλίσουν την ασφάλεια των πολύτιμων δεδομένων των πελατών τους. Και για τις πολύ μικρές επιχειρήσεις όπως και για τις μικρομεσαίες, η ασφάλεια των δεδομένων αποτελεί την πρώτη πρόκληση που πρέπει να αντιμετωπίσουν. Ωστόσο, στο 49% των πολύ μικρών επιχειρήσεων και στο 64% των μικρομεσαίων επιχειρήσεων, τα πολύτιμα δεδομένα πελατών αποθηκεύονται στις φορητές συσκευές των μελών του προσωπικού. Η διαρροή των δεδομένων αυτών μπορεί να έχει ως αποτέλεσμα σοβαρή ζημία στη φήμη της εταιρείας, καθώς και οικονομικές ζημίες που προκύπτουν από δικαστικές διαφορές. Ενώ οι μεγάλες επιχειρήσεις έχουν κατά κανόνα αποθεματικούς πόρους για να αντιμετωπίσουν τέτοιες δυσκολίες, οι μικρότεροι οργανισμοί ενδέχεται να αντιμετωπίσουν δραματικές συνέπειες, όπως σοβαρές διαταραχές στις λειτουργίες ή ακόμη και απώλειες πελατών.

Αν και οι μικρές εταιρείες συνειδητοποιούν το πρόβλημα, δεν έχουν κατανοήσει σαφώς το ποιος φέρει την ευθύνη για αυτά τα

περιουσιακά στοιχεία, δεδομένου ότι υποβάλλονται σε επεξεργασία από τις υπηρεσίες cloud. Οι εταιρείες με έως και 49 μέλη προσωπικό δείχνουν μια ιδιαίτερα ανησυχητική στάση απέναντι σε αυτό το πρόβλημα. Για παράδειγμα, σχεδόν τα δύο τρίτα (64%) των ερωτηθέντων που εργάζονται σε πολύ μικρές επιχειρήσεις είναι πεπεισμένοι ότι ο πάροχος είναι υπεύθυνος για την ασφάλεια των εφαρμογών ανταλλαγής εγγράφων, ενώ το 56% των ερωτηθέντων που εργάζονται σε μικρομεσαίες επιχειρήσεις συμμερίζονται την ίδια άποψη.

«Για να απολαύσουν τα πλεονεκτήματα του cloud computing ανεξάρτητα από το στάδιο ανάπτυξης που βρίσκονται, οι επιχειρήσεις πρέπει να διαχειριστούν αποτελεσματικά μια σειρά από πλατφόρμες και υπηρεσίες cloud. Βασικό είναι να βρίσκονται σε θέση να αναγνωρίσουν με σαφήνεια ποιος είναι υπεύθυνος για την ψηφιακή ασφάλεια στις υποδομές πληροφορικής που συνεχίζουν να αυξάνονται σε πολυπλοκότητα. Είτε τις διαχειρίζεται εσωτερικό προσωπικό είτε αξιόπιστος σύμβουλος, η ψηφιακή ασφάλεια δεν μπορεί να αγνοηθεί», δήλωσε ο Maxim Frolov, Vice President of Global Sales στην Kaspersky Lab. *«Όλες οι επιχειρήσεις θα πρέπει επομένως να δημιουργήσουν έναν ειδικό ρόλο στο πλαίσιο του οποίου η ασφάλεια των cloud πλατφορμών, τα ευαίσθητα δεδομένα και οι επιχειρηματικές διαδικασίες θα παραμείνουν υπό έλεγχο».*

Για να διατηρηθεί η ψηφιακή ασφάλεια σε κάθε στάδιο ανάπτυξης της επιχείρησης, η Kaspersky Lab προσφέρει ένα χαρτοφυλάκιο λύσεων ειδικά σχεδιασμένων για οργανισμούς οποιουδήποτε μεγέθους – από μικρές επιχειρήσεις μέχρι ενεργά αναπτυσσόμενες και πιο ώριμες εταιρείες. Σύμφωνα με την αυξανόμενη τάση χρήσης των clouds, στο χαρτοφυλάκιο της Kaspersky Lab υπάρχουν λύσεις ασφάλειας που μπορούν να αναπτυχθούν και να διαχειριστούν από το cloud, καθώς και ειδικά προϊόντα για την προστασία εφαρμογών του.

Για περισσότερες λεπτομέρειες σχετικά με τις προκλήσεις που αντιμετωπίζουν οι μικρές και μεσαίες επιχειρήσεις καθώς μεγαλώνουν και αγκαλιάζουν τις cloud τεχνολογίες, μπορείτε να

διαβάσετε την πρόσφατη έκθεσή μας.

Το ανανεωμένο Kaspersky Safe Kids «λύνει τα χέρια» των γονέων κατά την περίοδο των διακοπών των Χριστουγέννων και όχι μόνο

Το 50% των γονέων πιστεύουν ότι οι ηλεκτρονικές απειλές για τα παιδιά τους αυξάνονται και ένας στους τρεις αισθάνεται ότι δεν έχει κανέναν έλεγχο στο τι βλέπουν ή τι κάνουν τα παιδιά του στο Διαδίκτυο. Κατά τη διάρκεια των σχολικών τους διακοπών, τα παιδιά έχουν ακόμα μεγαλύτερη ελευθερία και προθυμία να «βουτήξουν» στο Διαδίκτυο και να περάσουν τον χρόνο τους εκεί. Για να βοηθήσει τους γονείς να είναι ξένοιαστοι καθ' όλη τη διάρκεια των Χριστουγέννων και για να προστατέψει τους νεότερους χρήστες του Διαδικτύου από τις ηλεκτρονικές απειλές, η Kaspersky Lab παρουσίασε την επόμενη γενιά της υπηρεσίας Kaspersky Safe Kids. Πλέον, οι γονείς μπορούν να εμποδίζουν τις επικίνδυνες αιτήσεις αναζήτησης στις φορητές συσκευές των παιδιών τους, ενώ τα παιδιά μπορούν να βλέπουν πόσος χρόνος τους απομένει να εργαστούν στους υπολογιστές και να ζητήσουν από τους γονείς τους άδεια για περισσότερο χρόνο.

Το Kaspersky Safe Kids βοηθάει στην παρακολούθηση της

ασφάλειας των παιδιών στον πραγματικό και τον εικονικό κόσμο. Η λύση ειδοποιεί τους γονείς για τις πιθανές επικίνδυνες καταστάσεις στις οποίες μπορούν να βρεθούν τα παιδιά τους στο Διαδίκτυο, αποτρέπει διάφορα προβλήματα όπως την πρόσβαση σε ανεπιθύμητο περιεχόμενο και προσφέρει στους γονείς ψυχολογικές συμβουλές εάν χρειάζεται. Οι γονείς μπορούν να αποφασίσουν τι είναι ασφαλές για τα παιδιά τους και να προσαρμόσουν ανάλογα το Kaspersky Safe Kids μετά την εγκατάσταση της λύσης στα smartphones και τους υπολογιστές των παιδιών τους.

Για παράδειγμα, χωρίς τη διάσπαση του σχολείου, οι γονείς μπορούν να περιορίσουν τον χρόνο που μπορούν να ξοδέψουν τα παιδιά τους στις συσκευές – μετά την πάροδο αυτού του χρονοδιαγράμματος, ανάλογα με το λειτουργικό σύστημα και τις ρυθμίσεις που χρησιμοποιούνται, η πρόσβαση στη συσκευή μπορεί να αποκλειστεί αυτόματα ή το παιδί να λάβει την αντίστοιχη ειδοποίηση. Με τη βελτιωμένη έκδοση του Kaspersky Safe Kids, τα παιδιά μπορούν να δουν πόσο χρόνο έχουν ακόμα στους υπολογιστές τους, και εάν το επιθυμούν, μπορούν να ζητήσουν πρόσθετο χρόνο από την εφαρμογή Safe Kids. Ανάλογα με το πόσο καλά αισθάνονται, οι γονείς μπορούν να επιλέξουν να αποδεχτούν ή να απορρίψουν αυτό το αίτημα μέσω του προσωπικού τους «χώρου» στο portal My Kaspersky. Με τη νέα έκδοση του Kaspersky Safe Kids, οι γονείς μπορούν επίσης να δουν πόσο χρόνο έχουν ξοδέψει τα παιδιά τους σε συσκευές μέσω της «γονικής λειτουργίας» της εφαρμογής Safe Kids στα δικά τους smartphones ή tablets, χωρίς να χρειάζεται να επισκεφθούν το portal My Kaspersky.

Σύμφωνα με έρευνα της Kaspersky Lab, οι μισοί γονείς ανησυχούν ότι τα παιδιά τους θα συναντήσουν ακατάλληλο περιεχόμενο στο Διαδίκτυο και η λύση Kaspersky Safe Kids μπορεί να εμποδίσει ή να προειδοποιήσει τα παιδιά για δυνητικά επικίνδυνες ιστοσελίδες και εφαρμογές. Η λειτουργία ασφαλούς αναζήτησης έχει ανανεωθεί τόσο που οι γονείς μπορούν να κρύψουν συγκεκριμένο περιεχόμενο από τα αποτελέσματα των αναζητήσεων που κάνουν τα παιδιά τους στις φορητές τους συσκευές,

συμπεριλαμβανομένων ιστότοπων με περιεχόμενο για ενήλικες, βίαιο περιεχόμενο, ιστότοπους σχετικούς με αλκοόλ και καπνικά προϊόντα κ.α. Αυτό σημαίνει ότι ακόμα κι αν ένα παιδί εισάγει άθελά του ένα τέτοιο αίτημα σε μια μηχανή αναζήτησης, τα αποτελέσματά του θα φιλτραριστούν.

Για να διευκολυνθεί η επικοινωνία με τη λύση, το νέο Kaspersky Safe Kids είναι τώρα οπλισμένο με ένα εκπαιδευτικό χαρακτηριστικό στους ηλεκτρονικούς υπολογιστές και μια δοκιμαστική λειτουργία στην οποία οι γονείς μπορούν να δοκιμάσουν τα χαρακτηριστικά της δωρεάν για μια εβδομάδα. Μεταξύ των χαρακτηριστικών που προσφέρονται είναι η «τοποθεσία του παιδιού» (παρέχεται η δυνατότητα να ζητείται η τοποθεσία ενός παιδιού και να καθορίζονται τα όρια της τοποθεσίας για συγκεκριμένες ώρες της ημέρας, συμπεριλαμβανομένων ειδοποιήσεων εάν τα παιδιά ξεπερνούν τα όρια αυτά) και «διαχείριση κοινωνικών δικτύων» (όπου οι γονείς μπορούν να λαμβάνουν λεπτομερή στατιστικά σχετικά με τη δημόσια δραστηριότητα των παιδιών τους στο Διαδίκτυο).

«Το γεγονός ότι το μυαλό των παιδιών είναι εγγενώς ευεπηρέαστο σημαίνει ότι τα παιδιά είναι πολύ ευάλωτα σε απειλές και δυνητικά τραυματικό περιεχόμενο, με το οποίο ο κυβερνοχώρος είναι γεμάτος. Ως εκ τούτου, η διαδικτυακή προστασία των γονέων σήμερα είναι απαραίτητη και σίγουρα δεν πρέπει να αγνοηθεί, ειδικά κατά τις σχολικές διακοπές. Αποστολή της Kaspersky Lab είναι να σώσει τον κόσμο και τον καθένα από τους διαδικτυακούς κινδύνους, συμπεριλαμβανομένων των νεότερων χρηστών του Διαδικτύου. Αυτός είναι και ο λόγος που δημιουργήθηκε το Kaspersky Safe Kids», σχολιάζει ο Andrei Mochola, Head of Consumer Business της Kaspersky Lab.

Εδώ μπορείτε να βρείτε περισσότερες πληροφορίες για τη λύση Kaspersky Safe Kids.

Οι προβλέψεις της Kaspersky Lab για τις ψηφιακές απειλές του 2018

Τα επόμενα χρόνια, ο κόσμος θα δει ακόμα περισσότερα νόμιμα λογισμικά να «μολύνονται» από ομάδες που στοχεύουν σε ευρύτερα προφίλ θυμάτων και γεωγραφικές περιοχές, με το πρόσθετο πλεονέκτημα ότι τέτοιες επιθέσεις είναι εξαιρετικά δύσκολο να εντοπιστούν και να μετριαστούν, σύμφωνα με τις Προβλέψεις Στοχευμένων Απειλών της Kaspersky Lab για το 2018. Άλλες επιθέσεις που είναι δύσκολο να εμποδιστούν, όπως αυτές που αφορούν κακόβουλο λογισμικό high-end φορητών συσκευών, θα αυξηθούν επίσης, καθώς οι επιτιθέμενοι καταφεύγουν σε νέες μεθόδους για να παραβιάζουν ολοένα και πιο προστατευμένους στόχους.

Οι ετήσιες προβλέψεις προετοιμάζονται από τους ειδικούς της εταιρείας, αξιοποιώντας την έρευνα και την εμπειρία που αποκτήθηκε κατά τη διάρκεια του έτους. Για το 2018, η Kaspersky Lab έχει συμπληρώσει τις προβλέψεις στοχευμένων απειλών της Παγκόσμιας Ομάδας Έρευνας και Ανάλυσης, με μία σειρά προβλέψεων για βιομηχανικές και τεχνολογικές απειλές.

Κορυφαίες προβλέψεις εξελιγμένων

στοχευμένων απειλών για το 2018

Το 2017, οι επιθέσεις σε συστήματα εφοδιαστικής αλυσίδας, όπως οι Shadowpad και ExPetya, μας έδειξαν πόσο εύκολα το λογισμικό τρίτων μπορεί να χρησιμοποιηθεί για να καταφέρουν να εισέλθουν σε επιχειρήσεις. Αυτή η απειλή αναμένεται να αυξηθεί το 2018, καθώς μερικοί από τους πιο επικίνδυνους φορείς παγκοσμίως ξεκίνησαν να υιοθετούν αυτήν την προσέγγιση ως μία εναλλακτική στις τεχνικές τύπου watering hole ή επειδή άλλες προσπάθειες να διεισδύσουν απέτυχαν.

«Οι επιθέσεις σε συστήματα εφοδιαστικής αλυσίδας αποδεικνύονται κάθε φορά εφιαλτικές όπως είχαμε προβλέψει στο παρελθόν. Καθώς οι προηγμένοι φορείς απειλής εξακολουθούν να έχουν πρόσβαση σε ευάλωτες εταιρείες ανάπτυξης λογισμικού, το back dooring δημοφιλών ή τοπικών δημοφιλών λογισμικών θα γίνει όλο και πιο επιθυμητός φορέας επίθεσης. Οι επιθέσεις σε συστήματα εφοδιαστικής αλυσίδας θα επιτρέψουν στους επιτιθέμενους να αποκτήσουν επιτυχώς πρόσβαση σε πολλές επιχειρήσεις που αποτελούν μέρος του οικοσυστήματος-στόχου, ενώ το «ραντάρ» των διαχειριστών συστημάτων και των λύσεων ασφάλειας δεν θα μπορεί να τις εντοπίσει», δήλωσε ο Juan Andrés Guerrero-Saade, Principal Security Researcher της Παγκόσμιας Ομάδας Έρευνας και Ανάλυσης της Kaspersky Lab.

Οι υπόλοιπες προβλέψεις στοχευμένων απειλών για το 2018 περιλαμβάνουν:

- **Περισσότερα high-end mobile κακόβουλα λογισμικά.** Τα τελευταία δύο χρόνια, η κοινότητα της ασφάλειας έχει αποκαλύψει προηγμένο κακόβουλο λογισμικό για φορητές συσκευές, το οποίο, σε συνδυασμό με exploits, αποτελεί ένα ισχυρό όπλο εναντίον του οποίου δεν υπάρχει επαρκής προστασία.
- **Οι καταστροφικές επιθέσεις θα συνεχίσουν να αυξάνονται.** Οι επιθέσεις Shamoon0 και StoneDrill που αναφέρθηκαν στις αρχές του 2017 και η επίθεση ExPetr/NotPetya τον

Ιούνιο αποκάλυψαν την αυξανόμενη τάση για καταστροφικές επιθέσεις.

- **Περισσότερες επιθέσεις θα οδηγήσουν με αναγνωριστικό τρόπο και δημιουργία προφίλ στην προστασία των πιο πολύτιμων exploits των εισβολέων.** Οι επιτιθέμενοι θα σπαταλούν περισσότερο χρόνο στην αναγνώριση και θα χρησιμοποιούν εργαλεία δημιουργίας προφίλ, όπως το «BeEF» για να διαπιστώσουν αν μπορούν να χρησιμοποιήσουν ένα λιγότερο κοστοβόρο non-zero day exploit.
- **Θα ανακαλυφθούν εξελιγμένες επιθέσεις οι οποίες θα βρίσκουν τον τρόπο σύνδεσης μεταξύ λειτουργικού συστήματος και firmware.** Το Unified Extensible Firmware Interface (UEFI) είναι το λογισμικό διεπαφής ανάμεσα στο firmware και στο λειτουργικό σύστημα στους σύγχρονους υπολογιστές. Οι ειδικοί της Kaspersky Lab αναμένουν ότι περισσότεροι απειλητικοί φορείς θα κάνουν χρήση των εξαιρετικά προηγμένων δυνατοτήτων της UEFI για τη δημιουργία κακόβουλου λογισμικού, το οποίο θα μπορεί να εγκατασταθεί προτού καν οποιαδήποτε anti-malware λύση ή ακόμα και το ίδιο το λειτουργικό σύστημα προλάβουν να εκκινήσουν.
- **Περισσότερες παραβιάσεις router και modem**. Αυτός ο γνωστός τομέας ευπάθειας έχει αγνοηθεί σε μεγάλο βαθμό ως εργαλείο για προηγμένους στοχευμένους επιτιθέμενους. Βρίσκονται σε μια κρίσιμη συγκυρία για έναν εισβολέα που επιδιώκει να κερδίσει μόνιμη και μυστική πρόσβαση σε ένα δίκτυο, και θα μπορούσαν να επιτρέψουν σε έναν εισβολέα ακόμη και να κρύψει τα ίχνη του.

Παράλληλα με αυτές τις προβλέψεις προηγμένων απειλών, οι προβλέψεις της Kaspersky Lab αναφορικά με τις απειλές για τη βιομηχανία και την τεχνολογία στοχεύουν να βοηθήσουν ορισμένους από τους πλέον συνδεδεμένους τομείς να κατανοήσουν και να προετοιμαστούν για τις προκλήσεις ασφάλειας που θα μπορούσαν να αντιμετωπίσουν τους επόμενους 12 μήνες.

Οι κορυφαίες προβλέψεις απειλών του 2018 για τη βιομηχανία περιλαμβάνουν:

- Τα **συνδεδεμένα οχήματα** είναι πιθανό να αντιμετωπίσουν νέες απειλές εξαιτίας της αυξανόμενης πολυπλοκότητας της εφοδιαστικής αλυσίδας που οδηγεί σε ένα σενάριο όπου κανένας παίκτης δεν έχει ορατότητα του, πόσο μάλλον τον έλεγχο, ολόκληρο τον πηγαίο κώδικα ενός οχήματος. Αυτό θα μπορούσε να διευκολύνει τους εισβολείς να παραβιάζουν και να παρακάμπτουν την ανίχνευση.
- Στην **υγειονομική περίθαλψη**, οι επιθέσεις που παραβιάζουν ιδιωτικά δίκτυα για να στοχεύσουν τον ιατρικό εξοπλισμό και τα δεδομένα αποσκοπώντας σε εκβιασμούς και κακόβουλη δραστηριότητα, θα μπορούσαν να αυξηθούν καθώς αυξάνεται ο όγκος ειδικού ιατρικού εξοπλισμού που συνδέεται με δίκτυα υπολογιστών.
- Στις **χρηματοπιστωτικές υπηρεσίες**, η αυξημένη ασφάλεια των ηλεκτρονικών πληρωμών σημαίνει ότι οι απατεώνες θα στρέψουν την προσοχή τους σε επιθέσεις εξαγοράς λογαριασμού. Οι εκτιμήσεις της βιομηχανίας δείχνουν ότι η απάτη αυτού του τύπου θα ανέλθει σε δισεκατομμύρια δολάρια.
- Τα **συστήματα βιομηχανικής ασφάλειας** είναι πιθανό να διατρέχουν αυξημένο κίνδυνο στοχευμένων επιθέσεων με προγράμματα Τα λειτουργικά συστήματα τεχνολογίας είναι πιο ευάλωτα από τα εταιρικά δίκτυα πληροφορικής και συχνά εκτίθενται στο Διαδίκτυο.
- Η Kaspersky Lab αναμένει επίσης να δούμε στοχευμένες επιθέσεις σε εταιρείες με σκοπό την εγκατάσταση **cryptocurrency** miners – και με την πάροδο του χρόνου θα μπορούσε να γίνει μια πιο προσοδοφόρα, μακροπρόθεσμη επιχειρηματική πρόταση σε σύγκριση με το ransomware.

Οι πλήρεις προβλέψεις της Kaspersky Lab για τις ψηφιακές απειλές του 2018 είναι διαθέσιμες στον ειδικό ιστότοπο

Securelist.com.

Grey Saturday: η ασφαλέστερη μέρα των σούπερ εκπτώσεων το διάστημα μεταξύ Black Friday και Cyber Monday

Οι Black Friday/Cyber Monday προσφέρουν απίθανες ευκαιρίες, αλλά είναι επίσης ημέρες αιχμής για επιθέσεις οικονομικού phishing – και οι καταναλωτές είναι σημαντικά ασφαλέστεροι το «Grey Saturday», καθώς ο αριθμός των επιθέσεων μειώνεται έως και κατά το ένα τρίτο παρά το γεγονός ότι είναι κορυφαία ημέρα αγορών. Το Grey Saturday εντοπίστηκε κατά τη διάρκεια της ετήσιας επισκόπησης της Kaspersky Lab σχετικά με νέες επιθέσεις οικονομικού phishing που εντοπίστηκαν κατά τη διάρκεια της εορταστικής εκπτωτικής περιόδου.

Η επισκόπηση της Kaspersky Lab διαπίστωσε σημάδια μείωσης των επιθέσεων το Grey Saturday τόσο το 2016 όσο και το 2015. Το 2016, σημειώθηκε πτώση κατά 33% στον αριθμό των επιθέσεων που χρησιμοποιούν δημοφιλή εμπορικά σήματα λιανικής πώλησης και πληρωμής (από περίπου 770.000 στις 510.000 ανιχνεύσεις), παρόλο που αυτή είναι η δεύτερη μεγαλύτερη ημέρα αγορών σε ορισμένες χώρες, όπως οι ΗΠΑ.

Η αλλαγή στον αριθμό των επιθέσεων phishing που χρησιμοποιούν ονόματα δημοφιλών εμπορικών σημάτων, τραπεζών και πληρωμών κατά τη διάρκεια της εβδομάδας της Black Friday το 2015 και το 2016 (δεδομένα από όλα τα συστήματα ασφάλειας της Kaspersky Lab – ευρετικές,offline και cloud ανιχνεύσεις).

Αντιπροσωπεύει μια σπάνια στιγμή ανάπαυλας για τους ψηφιακούς εγκληματίες σε μια όλο και πιο δραστήρια εορταστική αγοραστική περίοδο που ξεκινάει από τον Οκτώβριο και φτάνει μέχρι τον Δεκέμβριο. Παραδοσιακά διανέμονται μέσω email, οι επιθέσεις phishing προσελκύουν πλέον τους καταναλωτές μέσω weblinks, banners, μέσα κοινωνικής δικτύωσης και πολλά άλλα, πείθοντάς τους να «αποχωριστούν» τα προσωπικά τους οικονομικά δεδομένα, πιστεύοντας ότι αντιμετωπίζουν μια αξιόπιστη και γνωστή μάρκα.

«Η αύξηση των χρηστών που πραγματοποιούν ηλεκτρονικές πληρωμές, τραπεζικές συναλλαγές και ηλεκτρονικές αγορές σημαίνει ότι οι επιθέσεις οικονομικού phishing είναι πλέον σταθερά αυξημένες καθ 'όλη τη διάρκεια του έτους, αλλά η εορταστική περίοδος καθιστά πολύ πιο εύκολη την απόκρυψη τους μέσα στον γενικότερο «θόρυβο». Αυτή τη στιγμή του χρόνου, τα επίπεδα μάρκετινγκ και διαφήμισης εκτινάσσονται και οι καταναλωτές πραγματοποιούν όλο και περισσότερο τις συναλλαγές τους στις φορητές τους συσκευές – πιθανώς ενώ βρίσκονται στο δρόμο και είναι βιαστικοί – σχεδόν όλοι είναι πιο εκτεθειμένοι και έχουν λιγότερο χρόνο να σκέφτονται και να ελέγχουν. Το Grey Saturday ο αριθμός των επιθέσεων μειώνεται σημαντικά. Τα Σαββατοκύριακα σημειώνονται γενικά λιγότεροι αριθμοί επιθέσεων και λιγότεροι άνθρωποι βρίσκονται online – αλλά αυτήν την κορυφαία ημέρα αγορών αυτό είναι ένα επιπλέον πλεονέκτημα. Αναμένουμε αυτή η τάση από το 2016 να συνεχιστεί το 2017, οπότε αν σκοπεύετε να ψωνίσετε online και φέτος, επιλέξτε την ημέρα με σύνεση», δήλωσε η Nadezhda Demidova, Lead Web-Content Analyst της Kaspersky Lab.

Άλλα ευρήματα της έκθεσης περιλαμβάνουν:

- Μετά από μια πτώση το 2015, το οικονομικό phishing που εκμεταλλεύεται τα ηλεκτρονικά συστήματα πληρωμών, τις τράπεζες και τα καταστήματα λιανικής αυξήθηκαν και πάλι το 2016.
- Το οικονομικό phishing αντιπροσωπεύει πλέον τις μισές (49,77%) επιθέσεις phishing, επίπεδα ανεβασμένα από 34,33% το 2015.

- Οι καταναλωτές που χρησιμοποιούν πρωτίστως φορητές συσκευές είναι πιθανό να αποτέλεσαν βασικό μοχλό για την άνοδο του οικονομικού phishing: η χρήση των smartphones για ηλεκτρονικές τραπεζικές συναλλαγές, πληρωμές και αγορές έχει διπλασιαστεί κατά το τελευταίο έτος σύμφωνα με τον Δείκτη Ψηφιακής Ασφάλειας της Kaspersky Lab για το
- Οι χρηματοοικονομικοί phishers εκμεταλλεύονται το όνομα της Black Friday στις επιθέσεις τους, καθώς και την ευαισθητοποίηση των καταναλωτών και τις ανησυχίες τους για την ασφάλεια στο Διαδίκτυο – παρουσιάζοντας τα μηνύματα της επίθεσής τους ως ειδοποιήσεις ασφάλειας, υπονοώντας ότι ο χρήστης έχει πέσει θύμα χάκερ ή προσθέτοντας καθησυχαστικά μηνύματα ασφάλειας.

Για να παραμείνετε προστατευμένοι ενώ πραγματοποιείτε ηλεκτρονικές αγορές – οποιαδήποτε ημέρα του έτους – η Kaspersky Lab συμβουλεύει τα ακόλουθα:

- Μην κλικάρετε σε links που λαμβάνετε από άγνωστες πηγές ή σε links που φαίνονται ύποπτα.
- Μην χρησιμοποιείτε απροστάτευτα δημόσια δίκτυα Wi-Fi για να πραγματοποιήσετε πληρωμές μέσω Διαδικτύου, καθώς τα hotspots μπορούν εύκολα να παραβιαστούν για να «ακούσουν» την κίνηση των χρηστών και να κλέψουν εμπιστευτικές πληροφορίες.
- Μην εισάγετε τα στοιχεία της πιστωτικής σας κάρτας σε άγνωστους ή ύποπτους ιστότοπους και ελέγχετε πάντα ότι η ιστοσελίδα είναι γνήσια πριν εισαγάγετε προσωπικά στοιχεία (τουλάχιστον ρίξτε μια ματιά στη διεύθυνση URL). Οι ψεύτικες ιστοσελίδες μπορεί να μοιάζουν με τις πραγματικές.
- Χρησιμοποιείτε μόνο ιστότοπους που εκτελούνται με ασφαλή σύνδεση – η διεύθυνση του ιστότοπου πρέπει να ξεκινά με το HTTPS: //.
- Όσο περισσότερες πληροφορίες σας ζητούνται, τόσο πιο προσεκτικοί θα πρέπει να είστε: αναρωτηθείτε αν

χρειάζονται πραγματικά όλες τις πληροφορίες που απαιτούν.

- Να θυμάστε ότι οι τράπεζες και οι εταιρείες πληρωμών δεν θα σας ζητήσουν ποτέ να εισαγάγετε όλα τα στοιχεία σύνδεσής σας. Σε περίπτωση αμφιβολίας, καλέστε τους.
- Εγκαταστήστε μια λύση ασφαλείας στη συσκευή σας με ενσωματωμένες τεχνολογίες που έχουν σχεδιαστεί για να αποτρέπουν οικονομικές απάτες. Για παράδειγμα, η τεχνολογία Safe Money στις λύσεις της Kaspersky Lab δημιουργεί ένα ασφαλές περιβάλλον για οικονομικές συναλλαγές σε όλα τα επίπεδα.

Η επισκόπηση της Kaspersky Lab για το χρηματοοικονομικό phishing κατά την εορταστική περίοδο βασίζεται σε πληροφορίες που συλλέγονται από το ευρετικό anti-phishing εργαλείο της Kaspersky Lab που ενεργοποιείται κάθε φορά που ένας χρήστης επιχειρεί να ανοίξει ένα phishing link που δεν έχει προστεθεί ακόμα στη βάση δεδομένων της Kaspersky Lab.

Για να μάθετε περισσότερα σχετικά με τις τελευταίες τάσεις και παραδείγματα phishing επιθέσεων, ανατρέξτε στην αναφορά απειλών της Kaspersky Lab «*Beyond Black Friday*» στον ειδικό ιστότοπο Securelist.

Η Kaspersky Lab παρουσιάζει

το Polys, ένα ασφαλές σύστημα ηλεκτρονικής ψηφοφορίας βασισμένο στην τεχνολογία blockchain

Η Kaspersky Lab, στο πλαίσιο του ετήσιου Συνεδρίου της Cyber Security Weekend, ανακοίνωσε μία καινοτομία που προήλθε από το Kaspersky Lab Business Incubator: Μία προσαρμόσιμη πλατφόρμα ηλεκτρονικής ψηφοφορίας για μη κερδοσκοπικούς οργανισμούς, επιχειρήσεις και κοινότητες, η οποία χρησιμοποιεί blockchain τεχνολογία και είναι ασφαλής διότι διαθέτει διαφανείς κρυπταλγόριθμους.

Η έννοια της online ψηφοφορίας προσελκύει πολλούς ενδιαφερόμενους στη σύγχρονη κοινωνία, όπως πανεπιστήμια, επιχειρήσεις και κοινότητες που θέλουν να «ακούσουν» τα μέλη τους – τα οποία βρίσκονται συχνά σε διαφορετικά γεωγραφικά σημεία ή δεν επιθυμούν να συμμετέχουν σε φυσική ψηφοφορία. Ωστόσο, ο κίνδυνος να πραγματοποιεί ο χρήστης κρίσιμες επιλογές για τη ζωή του online παραμένει μεγάλος, με της μεγάλης κλίμακας ηλεκτρονικές ψηφοφορίες να παρέχουν τεράστιες ευκαιρίες για τους ψηφιακούς εγκληματίες να χειραγωγήσουν τα αποτελέσματα. Κατά τη διάρκεια του Cyber Security Weekend, ένα πάνελ που συστάθηκε από ειδικούς της Kaspersky Lab, της Agriledger και της Richtopia είχε σαν κεντρικό θέμα το πώς μπορούμε να καταστήσουμε τη διαδικασία ασφαλή και να διασφαλίσουμε ότι οι ψήφοι μας δεν θα αλλάξουν ή δεν θα μεταβληθούν από εξωτερικούς ή εσωτερικούς παράγοντες.

Κατά τη διάρκεια των συζητήσεων, η Kaspersky Lab παρουσίασε το πειραματικό πρόγραμμα «Polys», ένα νέο εμπορικό προϊόν που δημιουργήθηκε από μία ομάδα προγραμματιστών του Business Incubator, το οποίο στοχεύει να παρέχει σε οποιονδήποτε τη δυνατότητα να πραγματοποιεί ασφαλή, ανώνυμη και κλιμακούμενη

ηλεκτρονική ψηφοφορία με αποτελέσματα που δεν μπορούν να τροποποιηθούν από συμμετέχοντες ή διοργανωτές.

Ο Vartan Minasyan, Head of Investment and Innovation της Kaspersky Lab σχολίασε: «*Στο Kaspersky Lab Business Incubator υποστηρίζουμε την ανάπτυξη νέων ιδεών και τεχνολογιών που προέρχονται τόσο από εσωτερικές όσο και εξωτερικές ομάδες, οι οποίες μπορούν να εφαρμοστούν σε διάφορους τομείς όπου η προστασία και η ασφάλεια αποτελούν σημαντικές παραμέτρους. Ένας τέτοιος τομέας είναι οι ηλεκτρονικές ψηφοφορίες και, μάλιστα, εξερευνώντας εκτενέστερα τις πιθανές υλοποιήσεις του blockchain, η ομάδα μας συνειδητοποίησε ότι αυτή η τεχνολογία σε συνδυασμό με την τεχνογνωσία της εταιρείας σε θέματα ψηφιακής ασφάλειας θα μπορούσαν να λύσουν βασικά προβλήματα που σχετίζονται με την ιδιωτικότητα, τη διαφάνεια και την ασφάλεια των ηλεκτρονικών ψηφοφοριών. Είμαστε ενθουσιασμένοι που ήμασταν σε θέση να δημιουργήσουμε ένα κατάλληλο περιβάλλον γι αυτήν την εσωτερική καινοτομία».*

Το Polys είναι βασισμένο σε έξυπνα συμβόλαια στο Ethereum (κάποιες φορές αναφέρεται και ως Blockchain 2.0) το οποίο επιτρέπει την εξακρίβωση της ψηφοφορίας και τη διεξαγωγή ψηφοφοριών με αποκεντρωμένο τρόπο. Τα πλεονεκτήματα ασφαλείας της blockchain ψηφοφορίας είναι σημαντικά:

- Σύμφωνα με την αποκεντρωμένη φύση του blockchain, η ακρίβεια της εκτέλεσης της ψηφοφορίας μπορεί να επιβεβαιωθεί από τους συμμετέχοντες στο δίκτυο. Όλα τα δεδομένα της ψηφοφορίας αποθηκεύονται όχι σε servers, αλλά σε μπλοκ πληροφοριών στους υπολογιστές όλων των συμμετεχόντων στο δίκτυο. Για να το διαγράψει, ένας χάκερ θα πρέπει να παραβιάσει όλους τους υπολογιστές και να αποκτήσει πρόσβαση στα μεμονωμένα σύνολα δεδομένων.
- Η τεχνολογία blockchain επιτρέπει σε έναν ψηφοφόρο να ελέγξει αν η ψήφος του έχει καταχωρηθεί σωστά και οποιαδήποτε αλλοίωση των αποτελεσμάτων θα γίνει αυτόματα εμφανής.
- Η διαφάνεια της τεχνολογίας blockchain διευκολύνει την

παρακολούθηση των ψήφων και την ολοκλήρωση ελέγχων ψηφοφορίας από ανεξάρτητα μέρη.
- Τέλος, δεν απαιτούνται επιπλέον πόροι ή η ανάγκη για φυσική παρουσία προσωπικού.

Μια επιπλέον καινοτομία της λύσης Polys είναι ότι εξαλείφει τους περιορισμούς που είναι εγγενείς σε άλλες λύσεις blockchain:

- Στο πλαίσιο του συστήματος ψηφοφορίας Polys, το blockchain κρυπτογραφείται και υποστηρίζεται με μαθηματικούς αλγορίθμους. Αυτοί συμβάλλουν στην εξασφάλιση ανωνυμίας, αποκρύπτουν ενδιάμεσα αποτελέσματα και εκτελούν υπολογισμούς στα κρυπτογραφημένα δεδομένα, κάτι που δεν μπορεί να γίνει σε άλλα συστήματα blockchain λόγω της κατανεμημένης και ανοικτής φύσης τους.
- Ο πηγαίος κώδικας του Polys είναι διαθέσιμος στο κοινό – επιτρέποντας σε οποιονδήποτε λάτρη της τεχνολογίας blockchain, δοκιμαστή διείσδυσης ή υποστηρικτή ηλεκτρονικής ψηφοφορίας να δοκιμάσει, να επαληθεύσει και να διερευνήσει την τεχνολογία πίσω από αυτό στο GitHub.

Η Jutta Steiner, συνιδρύτρια της Parity Technologies, υποστηρικτής και σύμβουλος στο έργο, σχολιάζει: «*Η Parity Technologies είναι ενθουσιασμένη που εμπλέκεται με το Polys ως την πλατφόρμα επιλογής τους για ένα τόσο καινοτόμο έργο. Η τεχνολογία blockchain εφαρμόζεται ολοένα και περισσότερο από έναν μεγάλο αριθμό βιομηχανιών και πιστεύουμε ότι η αποκέντρωση της διαδικασίας ψηφοφορίας θα διασφαλίσει μια δίκαιη διαδικασία και θα δημιουργήσει υψηλό επίπεδο εμπιστοσύνης στο σύστημα».*

Για όσους επιθυμούν να δοκιμάσουν την υπηρεσία, υπάρχει μια freemium προσφορά, διαθέσιμη σε όλους και εύκολη στη δημιουργία. Το Polys προσφέρει επίσης μια προσαρμοσμένη

πλατφόρμα, η οποία είναι πλήρως κλιμακούμενη, με χωρητικότητα χιλιάδων ψηφοφόρων και μπορεί να προσαρμοστεί σε συγκεκριμένες απαιτήσεις όσον αφορά την εξουσιοδότηση, το σχεδιασμό διεπαφών και την ενσωμάτωση σε άλλες υπηρεσίες.

Περισσότερες πληροφορίες για τη λύση και την τεχνολογία μπορείτε να βρείτε στην ειδική ιστοσελίδα.

Σπάζοντας τη φούσκα του bitcoin: Οι spammers εξαργυρώνουν την ευφορία της τεχνολογίας blockchain

Ενώ οι κάτοχοι cryptocurrency αναζητούν νέες επενδυτικές ευκαιρίες και τρόπους για να αυξήσουν τις αποταμιεύσεις τους και οι λάτρεις ψάχνουν να μάθουν περισσότερα για τα οφέλη της μετάβασης σε συναλλαγές χωρίς μετρητά, οι κακόβουλοι χρήστες αναζητούν επίσης τρόπους αξιοποίησης της δημοτικότητας του φαινομένου blockchain. Πολλαπλοί μηχανισμοί απάτης με θέμα την τεχνολογία blockchain που εκμεταλλεύονται τη δημοσιότητα γύρω από την τεχνολογία αυτή έχουν εντοπιστεί πρόσφατα ελεύθεροι στο Διαδίκτυο, σύμφωνα με την έκθεση της Kaspersky Lab «Spam and phishing in Q3 2017».

Για αρκετούς μήνες, οι αποστολείς spam αλληλογραφίας παρουσιάζουν αυξημένη ευρηματικότητα, με τις δραστηριότητές

τους να αποδεικνύουν ότι παρακολουθούν τις τελευταίες τάσεις και τις παγκόσμιες εξελίξεις στα cryptocurrencies. Με βάση την τεχνολογία blockchain, τα cryptocurrencie έχουν γίνει ένας ελκυστικός στόχος για τους ψηφιακούς εγκληματίες, οι οποίοι έχουν στοχεύσει με επιτυχία και επιθετικά τα θύματά τους μέσω της «διαδικτυακής εξόρυξης» (web-mining). Παράλληλα, κατά τη διάρκεια των τελευταίων τριών μηνών, οι ερευνητές της Kaspersky Lab έχουν επίσης εντοπίσει αύξηση των δραστηριοτήτων spam που σχετίζονται με την κρυπτογράφηση. Σύμφωνα με την αναφορά «Spam and phishing in Q3 2017», οι εγκληματίες έχουν χρησιμοποιήσει αρκετά επιτυχημένα κόλπα για να ξεγελάσουν τους χρήστες και να κλέψουν τα χρήματά τους.

Οι μηχανισμοί απάτης, που βασίζονται στις συναλλαγές με cryptocurrency, έχουν επικρατήσει κατά το τελευταίο τρίμηνο. Σε ένα τέτοιο σενάριο, οι χρήστες λαμβάνουν μια πρόσκληση μέσω email για την εγκατάσταση ειδικού λογισμικού συναλλαγών με cryptocurrency, αλλά όταν πατούν το link, ανακατευθύνονται σε διαφορετικές ιστοσελίδες που προωθούν επενδυτικές επιλογές, συμπεριλαμβανομένων binary options συναλλαγών. Ωστόσο, για το θύμα δεν υπάρχει εγγύηση ότι αυτό θα οδηγήσει σε κάτι θετικό ή ότι θα πάρει τα χρήματά του πίσω. Αυτός ο τύπος μηχανισμού απάτης είναι παρόμοιος με το set-up των καζίνο και αποσκοπεί στο να προκαλέσει τους χρήστες να κάνουν προσφορές έως ότου δεν τους έχει μείνει τίποτα, αφήνοντας στους ψηφιακούς εγκληματίες τα πάντα.

Πιο απαρχαιωμένες, αλλά όχι λιγότερο αποτελεσματικές, τακτικές που χρησιμοποιούνται για την εκμετάλλευση θυμάτων περιλαμβάνουν τη διανομή email που προσφέρουν τη μεταφορά χρημάτων σε ένα συγκεκριμένο κρυπτογραφημένο πορτοφόλι, όπου ο χρήστης θα λαμβάνει τα χρήματά του πίσω. Αλλά, φυσικά, αυτό δεν συμβαίνει ποτέ. Οι χρήστες αρχικά μεταφέρουν τα χρήματα σε ένα άγνωστο πορτοφόλι και οι ψηφιακοί εγκληματίες τα εξαργυρώνουν.

Ένας άλλος μηχανισμός εξαπάτησης, που ανακαλύφθηκε από τους ερευνητές της Kaspersky Lab το τρίτο τρίμηνο, ήταν με τη μορφή

προσφοράς για να βοηθήσει τους χρήστες να μάθουν περισσότερα για τα cryptocurrencies και πώς θα μπορούσαν να επωφεληθούν από αυτά. Αυτή η ύπουλη τακτική είχε ως στόχο να εκμεταλλευτεί την έλλειψη κατανόησης σχετικά με την τεχνολογία blockchain και του τρόπου που λειτουργούν τα cryptocurrencies. Οι εγκληματίες διαφημίζουν εκπαιδευτικά εργαστήρια μέσω email που θα βοηθούσαν τους χρήστες να βελτιώσουν τις γνώσεις και τις δεξιότητές τους γύρω από τα cryptocurrencies και να ενημερωθούν για επενδυτικές ευκαιρίες. Με μια υψηλή τιμή, οι χρήστες εξαπατήθηκαν και πλήρωσαν πιστεύοντας ότι αυτή ήταν μια νόμιμη αγγελία. Ωστόσο, τα χρήματα που κατέβαλαν για να λάβουν τέτοιου είδους συμβουλές κατέληξαν να εμπλουτίζουν το πορτοφόλι κάποιου άλλου, και όχι τη γνώση του χρήστη. Κι αυτό γιατί συνήθως τέτοια εργαστήρια που προωθούνται μέσω spam email είναι αρκετά δαπανηρά και συνεπάγονται περισσότερη διαφήμιση παρά πραγματική γνώση.

«Ενώ κατά το δεύτερο τρίμηνο του έτους παρατηρήσαμε τις επιθέσεις spam και phishing του WannaCry, τους τελευταίους τρεις μήνες διαπιστώσαμε εγκληματίες που εκμεταλλεύονται ενεργά τη δημοτικότητα και το ενδιαφέρον γύρω από το cryptocurrency. Αυτό δείχνει για άλλη μια φορά ότι ο πιο αξιόπιστος τρόπος για να στοχεύουν τα θύματα είναι να αξιοποιούν τις τρέχουσες τάσεις και να εξαργυρώνουν μια αναδυόμενη αγορά την οποία οι χρήστες δεν έχουν κατανοήσει πλήρως και επιθυμούν να διερευνήσουν. Δεν υπάρχει αμφιβολία ότι οι επιθέσεις σε αυτή τη μορφή θα συνεχιστούν, οπότε είναι εξαιρετικά σημαντικό για τους χρήστες να δίνουν ιδιαίτερη προσοχή και να ενημερώνονται όταν πρόκειται για παγκόσμιο φαινόμενο», δήλωσε η Darya Gudkova, Spam Analyst Expert της Kaspersky Lab.

Μαζί με την αύξηση των blockchain απατών, ο μέσος όρος των spam email έχει αυξηθεί στο 58,02%, μέγεθος 1,05 ποσοστιαίες μονάδες υψηλότερο σε σύγκριση με το δεύτερο τρίμηνο. Σύμφωνα με την έκθεση, η μέγιστη δραστηριότητα spam email πραγματοποιήθηκε τον Σεπτέμβριο και άγγιξε το 59,56%.

Επιπλέον, κατά το τρίτο τρίμηνο του έτους οι ερευνητές ανίχνευσαν αύξηση των επιθέσεων phishing κατά 13 εκατομμύρια – το σύστημα Kaspersky Lab Anti-Phishing ενεργοποιήθηκε 59.569.508 φορές στους υπολογιστές των χρηστών της Kaspersky Lab. Ταυτόχρονα, οι εγκληματίες έχουν επικεντρωθεί περισσότερο στη χρήση εφαρμογών messenger σε φορητές συσκευές για την πραγματοποίηση δημοφιλών διαδικτυακών απατών.

Η αναλογία του spam στην κίνηση των email το 2ο τρίμηνο του 2017 σε σύγκριση με το τρίτο τρίμηνο

Άλλες σημαντικές τάσεις και στατιστικά στοιχεία για το τρίτο τρίμηνο που επισημάνθηκαν από τους ερευνητές της Kaspersky Lab, περιλαμβάνουν τα εξής:

- Η Κίνα έγινε η πιο δημοφιλής πηγή spam, ξεπερνώντας το Βιετνάμ και τις Η.Π.Α. Στις υπόλοιπες 10 χώρες περιλαμβάνονται η Ινδία, η Γερμανία, η Βραζιλία, η Γαλλία, η Πολωνία και η Ισλαμική Δημοκρατία του Ιράν.
- Η χώρα που αποτέλεσε στόχο κακόβουλων αποστολών email τις περισσότερες φορές ήταν η Γερμανία. Ο κορυφαίος στόχος της προηγούμενης περιόδου, η Κίνα ήρθε δεύτερη, ακολουθούμενη από τη Ρωσία, την Ιαπωνία και την Ιταλία.
- Το μεγαλύτερο ποσοστό χρηστών που επηρεάστηκαν από phishing email ήταν στη Βραζιλία (19,95%), όπως και το προηγούμενο τρίμηνο. Συνολικά, το 9,49% μοναδικών χρηστών προϊόντων της Kaspersky Lab παγκοσμίως δέχτηκαν επίθεση phishing.
- Οι κύριοι στόχοι επιθέσεων phishing παρέμειναν οι ίδιοι από την αρχή του έτους. Πρόκειται κυρίως για τον χρηματοπιστωτικό τομέα και περιλαμβάνονται οι τράπεζες, οι υπηρεσίες πληρωμών και τα ηλεκτρονικά καταστήματα.

Περισσότερες πληροφορίες σχετικά με το spam και το phishing το τρίτο τρίμηνο του 2017 μπορείτε να βρείτε στον ειδικό ιστότοπο Securelist.com.

Η Kaspersky Lab συνιστά στους οικιακούς χρήστες να

εγκαταστήσουν μια αξιόπιστη λύση ασφάλειας για την ανίχνευση και την παρεμπόδιση spam μηνυμάτων και επιθέσεων phishing, όπως η λύση Kaspersky Total Security.

Στις επιχειρήσεις συνιστάται να χρησιμοποιούν λύσεις ασφάλειας με αποκλειστική λειτουργικότητα που στοχεύει στην ανίχνευση και την παρεμπόδιση phishing επιθέσεων, κακόβουλων συνημμένων και spam μηνυμάτων. Οι μικρές επιχειρήσεις μπορούν να προστατευθούν με τις λύσεις Kaspersky Small Office Security και Kaspersky Endpoint Security Cloud, ενώ οι μεγαλύτερες εταιρείες μπορούν να επωφεληθούν από την cloud-assisted anti-spam σάρωση όλων των μηνυμάτων σε πραγματικό χρόνο, με την εφαρμογή Kaspersky Security for Mail Server που περιλαμβάνεται στη λύση Kaspersky Total Security for Business.

Για να διασφαλίσουμε ότι θα συνεχίσουμε να παρέχουμε τα υψηλότερα επίπεδα προστασίας στους πελάτες μας, η Kaspersky Lab θα παρουσιάσει το 2018 το Kaspersky Security for Office 365, μια νέα υπηρεσία Security-as-a-Service που παρέχει βραβευμένη προστασία από spam αλληλογραφία, phishing και κακόβουλο λογισμικό, για το Exchange online στο Microsoft Office 365. Το προϊόν διατίθεται προς το παρόν δημόσια σε beta έκδοση και θα συνεχίσει να διατίθεται δωρεάν μέχρι τον Φεβρουάριο του 2018.

Η Kaspersky Lab και το

Συμβούλιο της Ευρώπης συνεργάζονται για την προστασία των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο

Σύμφωνα με αναφορές, το 50% του παγκόσμιου πληθυσμού είναι συνδεδεμένο στο Διαδίκτυο και το ποσοστό αυτό συνεχώς αυξάνεται. Ο ψηφιακός κόσμος παίζει τόσο σημαντικό ρόλο στη ζωή των περισσότερων ανθρώπων και κατ' επέκταση θα πρέπει τα ανθρώπινα δικαιώματα να προστατεύονται και όχι – όπως συμβαίνει στην πραγματικότητα – να καταπατώνται διαρκώς. Το Συμβούλιο της Ευρώπης, θέλοντας να βελτιώσει αυτήν την κατάσταση, υπέγραψε σήμερα συμφωνία με την Kaspersky Lab και άλλες εταιρείες τεχνολογίας, με κοινή δέσμευση την προαγωγή του ανοικτού και ασφαλούς Διαδικτύου.

Κατά τη διάρκεια τελετής στο Στρασβούργο, την πρώτη ημέρα του Παγκόσμιο Φόρουμ για την Δημοκρατία 2017 (World Forum for Democracy), ο Anton Shingarev, Αντιπρόεδρος Δημοσίων Υποθέσεων στην Kaspersky Lab, και ο Γενικός Γραμματέας του Συμβουλίου της Ευρώπης Thorbjørn Jagland υπέγραψαν τη συμφωνία, η οποία αποσκοπεί στην επέκταση της προστασίας των ανθρωπίνων δικαιωμάτων, της δημοκρατίας και του κράτους δικαίου στο Διαδίκτυο.

Μαζί με την Kaspersky Lab, εκπρόσωποι άλλων επτά κορυφαίων εταιρειών στον τομέα της τεχνολογίας υπέγραψαν τη συμφωνία, η οποία έλαβε τη μορφή ανταλλαγής επιστολών. Σε αυτές περιλαμβάνονται η Apple, η Deutsche Telekom, το Facebook, η Google, η Microsoft, η Orange και η Telefónica. Έξι από τους σημαντικότερους τεχνολογικούς συλλόγους παγκοσμίως δεσμεύθηκαν επίσης για την αφοσίωσή τους – ανάμεσα στις οποίες η Ένωση Βιομηχανιών Υπολογιστών και Επικοινωνιών (CCIA), η DIGITALEUROPE, η ευρωπαϊκή ψηφιακή συμμαχία ΜμΕ (European

Digital SME Alliance), ο Σύνδεσμος Ευρωπαϊκών Φορέων Εκμετάλλευσης Τηλεπικοινωνιακών Δικτύων (ETNO), η GSMA και η Πρωτοβουλία Παγκόσμιου Δικτύου (GNI).

Η συμφωνία συνεργασίας συγκαταλέγεται στις προτεραιότητες που καθορίζονται στη Στρατηγική του Συμβουλίου της Ευρώπης για τη Διακυβέρνηση του Διαδικτύου κατά την περίοδο 2016-2019, η οποία αποσκοπεί στην προστασία των χρηστών του Διαδικτύου μέσω της οικοδόμησης διαδικτυακής δημοκρατίας και της διασφάλισης της προστασίας των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο. Προκειμένου να επιτευχθούν αυτοί οι στόχοι, η ομάδα – η οποία είναι επίσης ανοικτή στη συνεργασία με άλλους εταίρους στο μέλλον – συμφώνησε να συνεργαστεί σε διάφορους βασικούς τομείς. Αυτοί περιλαμβάνουν μεταξύ άλλων:

- Την προστασία των παιδιών από τη σεξουαλική εκμετάλλευση και κακοποίηση.
- Την ελευθερία της έκφρασης στον διαδικτυακό κόσμο.
- Το δικαίωμα στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων.
- Την εκπαίδευση για δημοκρατική αγωγή των πολιτών.
- Την ισότητα των φύλων στον διαδικτυακό κόσμο.
- Την καταπολέμηση του εγκλήματος και της τρομοκρατίας στον κυβερνοχώρο.
- Τον πολιτισμό και την ψηφιοποίηση.

Ο Anton Shingarev δήλωσε: «*Το Διαδίκτυο είναι ένας μοναδικός τομέας – ένας χώρος για να συνδεόμαστε όλοι καθημερινά. Διαβάζουμε τα νέα και επισκεπτόμαστε τα μέσα κοινωνικής δικτύωσης, σχεδιάζουμε τις διακοπές μας και ψωνίζουμε ηλεκτρονικά – και αφήνουμε πίσω μας ένα τεράστιο ψηφιακό αποτύπωμα κάθε μέρα. Αλλά αυτός ο μοναδικός χώρος είναι υπό σοβαρή απειλή: οι ψηφιακοί εγκληματίες προσπαθούν να τον εκμεταλλευτούν και να τον καταχραστούν, οι τρομοκράτες το χρησιμοποιούν για να στρατολογήσουν νέο κόσμο και οι κυβερνήσεις είναι απασχολημένες προσπαθώντας να το ρυθμίσουν. Είμαστε στην ευχάριστη θέση να συνεργαστούμε με το Συμβούλιο της Ευρώπης και αυτή την ευρύτερη ομάδα οργανισμών με μεγάλη*

επιρροή, σε μια κοινή αποστολή να κάνουμε το Διαδίκτυο προστατευμένο και ασφαλές – έτσι ώστε όλοι να συνεχίσουμε να απολαμβάνουμε πλήρως την ψηφιακή μας ζωή».

Ο Δείκτης Ψηφιακής Ασφάλειας της Kaspersky Lab το πρώτο εξάμηνο του 2017

Η αλλαγή στις συνήθειες χρήσης του Διαδικτύου, η υπέρμετρη χρήση φορητών συσκευών, αλλά και η αδιάφορη στάση απέναντι στην ασφάλεια των συσκευών επισημάνθηκαν ως οι βασικοί τομείς που επηρεάστηκαν όσον αφορά στην ψηφιακή ασφάλεια σύμφωνα με τον πρόσφατο Δείκτη Ψηφιακής Ασφάλειας της Kaspersky Lab – ο οποίος αποτελείται από ένα σύνολο δεικτών που έχουν σχεδιαστεί για να αντικατοπτρίζουν τις αλλαγές στις συμπεριφορές των χρηστών του Διαδικτύου και τους κινδύνους που αντιμετωπίζουν. Στο πρώτο μισό του 2017, σύμφωνα με τον Δείκτη, οι χρήστες χρησιμοποίησαν ολοένα και περισσότερο τις φορητές τους συσκευές, οι μεγαλύτεροι ηλικιακά χρήστες αντιμετώπισαν ένα αυξημένο επίπεδο διαδικτυακών κινδύνων και ο αριθμός των επηρεαζόμενων χρηστών που προστατεύονται από λύσεις ασφάλειας έχει μειωθεί.

Ο Δείκτης Ψηφιακής Ασφάλειας της Kaspersky Lab βασίζεται στα αποτελέσματα παγκόσμιων online ερευνών σε χρήστες του διαδικτύου, που πραγματοποιούνται δύο φορές τον χρόνο από την Kaspersky Lab. Το πρώτο μισό του 2017, συμμετείχαν στην έρευνα

21.081 χρήστες από 32 χώρες και ηλικίας 16 ετών και άνω.

Η έρευνα διαπίστωσε ότι οι σύγχρονοι χρήστες χρησιμοποιούν πιο σπάνια υπολογιστές για τις ηλεκτρονικές τους δραστηριότητες, αλλά προτιμούν να χρησιμοποιούν φορητές συσκευές. Λαμβάνοντας ως παράδειγμα το email, το 78% των χρηστών έχει πρόσβαση στο email του από υπολογιστές, σε σύγκριση με το 87% τους προηγούμενους έξι μήνες. Το 67% το κάνει από τις φορητές συσκευές του, μέγεθος αυξημένο σε σύγκριση με το 59% κατά το δεύτερο εξάμηνο του 2016. Το ποσοστό των χρηστών που χρησιμοποιούν τις φορητές συσκευές τους για online αγορές έχει αυξηθεί στο 50% από 41% τους προηγούμενους έξι μήνες, ενώ το ποσοστό των χρηστών που πραγματοποιούν ηλεκτρονικές αγορές από τους υπολογιστές τους μειώθηκε από 80% σε 75%. Αυτή η τάση παρατηρείται στους περισσότερους τύπους ηλεκτρονικών δραστηριοτήτων που παρακολουθούνται στον Δείκτη.

Επιπλέον, για πρώτη φορά ύστερα από αρκετά χρόνια, ο μέσος αριθμός συσκευών ανά νοικοκυριό παρουσίασε ελαφρά μείωση – κυρίως λόγω της μείωσης του αριθμού των υπολογιστών ανά νοικοκυριό. Σήμερα, ένα μέσο νοικοκυριό έχει 6,2 συσκευές συνδεδεμένες στο Διαδίκτυο, σε σύγκριση με 6,3 το δεύτερο εξάμηνο του 2016.

Ταυτόχρονα, το ποσοστό των χρηστών με λύση ασφάλειας στις συσκευές τους έχει επίσης παρουσιάσει μείωση. Ενώ στα τέλη του 2016 μόνο το 39% των ερωτηθέντων δεν είχε προστατεύσει όλες τις συσκευές του, τώρα το 41% των χρηστών παραδέχεται ότι δεν διαθέτει καθόλου προστασία. Αυτό μπορεί να σχετίζεται με το γεγονός ότι οι χρήστες χρησιμοποιούν ολοένα και περισσότερο φορητές συσκευές τις οποίες, πολύ συχνά, αφήνουν χωρίς λύση προστασίας σε σύγκριση με τους υπολογιστές τους. Αυτή είναι μια επικίνδυνη τάση: οι χρήστες αντιμετωπίζουν κινδύνους κατά τη χρήση φορητών συσκευών και όσο περισσότερο τις χρησιμοποιούν για δραστηριότητες στο Διαδίκτυο τόσο μεγαλύτερος είναι ο κίνδυνος.

Από τις αρχές του 2017, οι βάσεις δεδομένων της Kaspersky Lab

έχουν απαριθμήσει πάνω από 20 εκατομμύρια κακόβουλα αντικείμενα που στοχεύουν σε συσκευές Android. Οι χρήστες Android αντιμετωπίζουν σήμερα προγράμματα ransomware που κρυπτογραφούν τα δεδομένα του χρήστη στο τηλέφωνό τους σε αντάλλαγμα για λύτρα. Επίσης, κακόβουλο λογισμικό που αποσκοπεί στην κλοπή χρημάτων από εφαρμογές mobile banking και ιστοσελίδες phishing που έχουν σχεδιαστεί για να αποκτήσουν παράνομη πρόσβαση στους λογαριασμούς ενός χρήστη, για παράδειγμα, στα κοινωνικά δίκτυα.

Ως αποτέλεσμα, κατά την εξεταζόμενη χρονική περίοδο, ένας στους τέσσερις (27%) ερωτηθέντες ανέφερε ότι έχει πέσει θύμα ψηφιακού εγκλήματος σε κάποιο είδος συσκευής. Αν και κατά μέσο όρο το ποσοστό αυτών των επηρεαζόμενων χρηστών έχει μειωθεί τους πρώτους 6 μήνες του έτους, αυτή η μείωση παρατηρήθηκε μόνο στους ερωτηθέντες που είχαν εγκαταστήσει λύσεις ασφαλείας στις συσκευές τους.

Οι μεγαλύτερης ηλικίας χρήστες (55 ετών και άνω) βρέθηκαν σε υψηλότερο κίνδυνο το πρώτο εξάμηνο του 2017. Ενώ το δεύτερο εξάμηνο του 2016 μόνο το 12% των χρηστών αυτών ανέφερε ότι αντιμετώπισε μια διαδικτυακή απειλή, το πρώτο εξάμηνο αντιμετώπισε κάποιου είδους κακόβουλο λογισμικό το 19%.

«Ανεξάρτητα από την ηλικία και το επάγγελμα των ανθρώπων, το επίκεντρο της ψηφιακής τους ζωής μετατοπίζεται ολοένα και περισσότερο σε φορητές συσκευές – οι άνθρωποι τους εμπιστεύονται με τα μυστικά, τα αρχεία, τις εμπιστευτικές πληροφορίες, τα χρήματά τους και άλλα πολλά. Ωστόσο, οι ψηφιακοί εγκληματίες μετατοπίζουν επίσης τις τακτικές τους και επιτίθενται όλο και περισσότερο σε φορητές πλατφόρμες. Επομένως, είναι επιτακτική ανάγκη τα σύγχρονα smartphones και tablets να είναι τόσο προστατευμένα όσο και οι υπολογιστές μας. Εκτός από τη διασφάλιση των δικών μας συσκευών, οι άνθρωποι πρέπει να φροντίσουν ο ένας τον άλλον και να βοηθήσουν τους φίλους και τα μέλη της οικογένειάς τους να πραγματοποιούν ασφαλή χρήση του Διαδικτύου για να μειώσουν τους κινδύνους που αντιμετωπίζουν», σχολιάζει ο Andrei

Mochola, Head of Consumer Business της Kaspersky Lab.

Για να αντιμετωπίσουν αυτές τις απειλές και να βοηθήσουν τους ανθρώπους να προστατεύσουν τις φορητές τους συσκευές και τους αγαπημένους τους από το ψηφιακό έγκλημα, η Kaspersky Lab ανέπτυξε τη λύση Kaspersky Internet Security for Android. Προστατεύει τα smartphones και τα tablet από επικίνδυνες εφαρμογές και ιστότοπους, διασφαλίζει την ιδιωτική ζωή των χρηστών χάρη στο φιλτράρισμα κλήσεων και κειμένων και μια αντικλεπτική λειτουργία προστατεύει την ασφάλεια των δεδομένων του χρήστη σε περίπτωση που η συσκευή χαθεί ή κλαπεί.

Για περισσότερες πληροφορίες σχετικά με τον Δείκτη Ψηφιακής Ασφάλειας της Kaspersky και τη συμπεριφορά των χρηστών όταν βρίσκονται online σε διάφορες χώρες, ηλικίες και φύλα, επισκεφτείτε τη διεύθυνση http://index.kaspersky.com.

Πάνω από όλα η εμπιστοσύνη: Παγκόσμια Πρωτοβουλία Διαφάνειας από την Kaspersky Lab

Η Kaspersky Lab ανακοινώνει την έναρξη της Παγκόσμιας Πρωτοβουλίας Διαφάνειας (*Global Transparency Initiative)* ως μέρος της διαρκούς της δέσμευσης για την προστασία των πελατών της από ψηφιακές απειλές, ανεξάρτητα από την προέλευση ή τον

σκοπό τους. Με την πρωτοβουλία αυτή, η Kaspersky Lab θα εμπλέξει την ευρύτερη κοινότητα ασφάλειας πληροφοριακών συστημάτων και άλλους ενδιαφερόμενους φορείς στην επικύρωση και επαλήθευση της αξιοπιστίας των προϊόντων της, των εσωτερικών διαδικασιών και των επιχειρηματικών δραστηριοτήτων της, καθώς και στην εισαγωγή πρόσθετων μηχανισμών λογοδοσίας, με τους οποίους η εταιρεία μπορεί να αποδείξει ότι αντιμετωπίζει άμεσα και αποτελεσματικά οποιοδήποτε πρόβλημα ασφάλειας. Ως μέρος της πρωτοβουλίας, η εταιρεία σκοπεύει να παρέχει τον πηγαίο κώδικα του λογισμικού της – συμπεριλαμβανομένων ενημερώσεων λογισμικού και ενημερώσεων κανόνων ανίχνευσης απειλών – για ανεξάρτητη αναθεώρηση και αξιολόγηση.

Καθώς η κοινωνία σήμερα εξαρτάται περισσότερο από τις τεχνολογίες της πληροφορικής και των επικοινωνιών (ΤΠΕ), οι ψηφιακές απειλές συνεχίζουν να πολλαπλασιάζονται και να εξελίσσονται. Λόγω του φρενήρη ρυθμού ανάπτυξης τόσο των ΤΠΕ όσο και του τοπίου απειλών, η Kaspersky Lab πιστεύει ότι η συνεργασία στο θέμα της προστασίας του κυβερνοχώρου είναι πιο σημαντική από ποτέ. Η εμπιστοσύνη είναι απαραίτητη για την ψηφιακή ασφάλεια και, επομένως, η εμπιστοσύνη πρέπει να αποτελεί τον θεμέλιο λίθο για οποιαδήποτε συνεργασία μεταξύ εκείνων που επιδιώκουν να προστατεύσουν από τις ψηφιακές απειλές τους χρήστες, τους οργανισμούς και τις επιχειρήσεις. Ωστόσο, η Kaspersky Lab αναγνωρίζει ότι η εμπιστοσύνη δεν είναι δεδομένη, πρέπει να κερδίζεται επανειλημμένα μέσω μιας διαρκούς δέσμευσης για διαφάνεια και ανάληψη ευθυνών.

Η Παγκόσμια Πρωτοβουλία Διαφάνειας της Kaspersky Lab είναι μια επιβεβαίωση της δέσμευσης της εταιρείας να κερδίζει και να διατηρεί την εμπιστοσύνη των πελατών και των συνεργατών της καθημερινά. Η εταιρεία δεν έχει θεωρήσει ποτέ αυτήν την εμπιστοσύνη δεδομένη, αλλά προσπαθεί συνεχώς να βελτιώνεται με κάθε δυνατό τρόπο.

Η αρχική φάση της Παγκόσμιας Πρωτοβουλίας Διαφάνειας της Kaspersky Lab θα περιλαμβάνει:

- Την έναρξη ενός ανεξάρτητου ελέγχου του πηγαίου κώδικα της εταιρείας έως το πρώτο τρίμηνο του 2018, με παρόμοιους ελέγχους των ενημερώσεων λογισμικού της εταιρείας και των κανόνων ανίχνευσης απειλών να ακολουθούν.
- Την έναρξη ανεξάρτητης αξιολόγησης (i) των διαδικασιών ασφαλούς ανάπτυξης του κύκλου ζωής της εταιρείας και (ii) των στρατηγικών άμβλυνσης των κινδύνων για το λογισμικό και την εφοδιαστική αλυσίδα της, μέχρι το πρώτο τρίμηνο του 2018.
- Την ανάπτυξη πρόσθετων ελέγχων που θα διέπουν τις πρακτικές επεξεργασίας δεδομένων της εταιρείας σε συντονισμό με ένα ανεξάρτητο φορέα που θα πιστοποιεί τη συμμόρφωση της εταιρείας με τους εν λόγω ελέγχους μέχρι το πρώτο τρίμηνο του 2018.
- Δημιουργία τριών Κέντρων Διαφάνειας παγκοσμίως, με σχέδια για τη δημιουργία του πρώτου το 2018, για την αντιμετώπιση οποιωνδήποτε ζητημάτων ασφάλειας από κοινού με πελάτες, αξιόπιστους εταίρους και κυβερνητικούς φορείς. Τα κέντρα θα δώσουν σε αξιόπιστους εταίρους της εταιρείας εύκολη πρόσβαση σε αξιολογήσεις του κώδικα της εταιρείας, σε ενημερώσεις λογισμικού και κανόνες ανίχνευσης απειλών, καθώς και άλλες δραστηριότητες. Τα Κέντρα Διαφάνειας θα ανοίξουν στην Ασία, την Ευρώπη και τις ΗΠΑ μέχρι το 2020.
- Η αύξηση των bug bounty αμοιβών οι οποίες αγγίζουν μέχρι και τα $100.000 για τις πιο σοβαρές ευπάθειες που εντοπίστηκαν στο πρόγραμμα Συντονισμένης Αποκάλυψης Ευπάθειας (Coordinated Vulnerability Disclosure) της εταιρείας για περαιτέρω ενθάρρυνση ανεξάρτητων ερευνητών ασφάλειας να συμπληρώσουν τις προσπάθειες ανίχνευσης και μετριασμού ευπαθειών μας μέχρι το τέλος του 2017.

Εκτός από την έναρξη αυτής της αρχικής φάσης της Παγκόσμιας Πρωτοβουλίας Διαφάνειας, η Kaspersky Lab προσβλέπει στη συνεργασία με ενδιαφερόμενους φορείς και την κοινότητα ασφάλειας του τομέα της Πληροφορικής για να καθορίσει ποια θα

πρέπει να είναι η επόμενη φάση της πρωτοβουλίας – ξεκινώντας από το δεύτερο εξάμηνο του 2018. Προτάσεις για περαιτέρω βήματα και αιτήσεις από τρίτα μέρη που ενδιαφέρονται να συνεργαστούν με την εταιρεία, είναι ευπρόσδεκτα στη διεύθυνση: transparency@kaspersky.com.

Αναφερόμενος στην ανάγκη για αυτή τη νέα πρωτοβουλία, ο Eugene Kaspersky, Πρόεδρος και Διευθύνων Σύμβουλος της Kaspersky Lab, δήλωσε: *«Η βαλκανοποίηση του Διαδικτύου δεν ωφελεί κανέναν παρά μόνο τους ψηφιακούς εγκληματίες. Η μειωμένη συνεργασία μεταξύ των χωρών βοηθά τους κακούς στις δραστηριότητές τους και οι συμπράξεις δημοσίου και ιδιωτικού τομέα δεν λειτουργούν όπως πρέπει. Το Διαδίκτυο δημιουργήθηκε για να ενώσει τους ανθρώπους και να μοιραστεί η γνώση. Η ψηφιακή ασφάλεια δεν έχει σύνορα, αλλά η προσπάθεια εισαγωγής εθνικών συνόρων στον κυβερνοχώρο είναι αντιπαραγωγική και πρέπει να σταματήσει. Πρέπει να αποκαταστήσουμε την εμπιστοσύνη στις σχέσεις μεταξύ εταιρειών, κυβερνήσεων και πολιτών. Αυτός είναι ο λόγος για τον οποίο δρομολογούμε την Παγκόσμια Πρωτοβουλία Διαφάνειας: θέλουμε να δείξουμε ότι είμαστε απόλυτα ανοιχτοί και διαφανείς. Δεν έχουμε τίποτα να κρύψουμε. Και πιστεύω ότι με αυτές τις ενέργειες θα μπορέσουμε να ξεπεράσουμε τη δυσπιστία και να υποστηρίξουμε τη δέσμευσή μας να προστατεύσουμε τους ανθρώπους σε οποιαδήποτε χώρα του πλανήτη μας!»*

Η Kaspersky Lab θα μοιράζεται τακτικά λεπτομέρειες της προόδου της Πρωτοβουλίας και των πρόσθετων δραστηριοτήτων της. Συνεργαζόμενη με διάφορα ενδιαφερόμενα μέρη, η Kaspersky Lab ελπίζει ότι οι πελάτες και οι συνεργάτες της θα συμμετάσχουν σε αυτό το ταξίδι.

Εδώ μπορείτε να βρείτε περισσότερες πληροφορίες σχετικά με τις αρχές διαφάνειας της Kaspersky Lab: https://www.kaspersky.com/about/transparency