Η Kaspersky Lab κυκλοφορεί μια σημαντική ενημέρωση της πλατφόρμας της κατά των στοχευμένων επιθέσεων

Η Kaspersky Lab ανακοίνωσε την κυκλοφορία της ανανεωμένης πλατφόρμας Kaspersky Anti Targeted Attack Platform, μία λύση που εντοπίζει εξελιγμένες απειλές και στοχευμένες επιθέσεις εναντίον επιχειρήσεων. Η λύση συνδυάζει εξελιγμένους αλγόριθμους μηχανικής μάθησης, χειροπιαστή παγκόσμια πληροφόρηση για απειλές, προσαρμοστικότητα στις υποδομές των πελατών, ώστε να βοηθήσει μεγάλες επιχειρήσεις να αποκαλύψουν τις πιο εξελιγμένες και επικίνδυνες επιθέσεις σε οποιοδήποτε επίπεδο της ανάπτυξή τους. Η νέα πλατφόρμα Kaspersky Anti Targeted Attack Platform διαθέτει επίσης βελτιώσεις επεκτασιμότητας με ομαδοποιήσεις στο sandbox και βελτιστοποιημένη ορατότητα με σημαντικές ενημερώσεις στο γραφικό περιβάλλον χρήστη (GUI).

Η πλατφόρμα Kaspersky Anti Targeted Attack Platform συνδυάζει δικτυωμένους και τερματικούς αισθητήρες, τεχνολογία sandbox και έξυπνη ανάλυση για τη συσχέτιση διαφόρων δεικτών συμβιβασμού, αλλά και για να βοηθήσει τις επιχειρήσεις να ανακαλύψουν ακόμα και τις πιο πολύπλοκες στοχευμένες επιθέσεις. Για την αντιμετώπιση των πιο εξελιγμένων ψηφιακών απειλών, οι πιο πρόσφατες βελτιωμένες λύσεις φέρνουν νέα ισχυρά εργαλεία, όπως η παρακολούθηση της ροής της εργασίας, συμπεριλαμβάνοντας την κίνηση των emails και του διαδικτύου,

όταν ενσωματώνεται με τη λύση Kaspersky Security for Mail Gateway.

Νέα χαρακτηριστικά που ανταποκρίνονται σε συγκεκριμένες απαιτήσεις πελατών

O Oleg Glebov, Anti Targeted Attacks Solution Business Lead της Kaspersky Lab, σχολιάζει*: «Σύμφωνα με το στρατηγικό μας όραμα αναφορικά με την αποδοτική προσαρμογή της ασφάλειας των επιχειρήσεων, παρουσιάσαμε τρεις κύριους τομείς βελτίωσης του προϊόντος μας. Η πρώτη και σημαντικότερη βελτίωση είναι η προσθήκη νέων εργασιακών σεναρίων με στόχο τη βελτίωση της συνολικής ορατότητας, τις δυνατότητες ανάλυσης και τη συσχέτιση διαφόρων περιστατικών που πιθανώς να συνδέονται με ένα μόνο συμβάν. Δεύτερη έρχεται η προσθήκη νέων επεκτάσεων, ευελιξίας και ικανότητας προσαρμογής σε μοναδικές απαιτήσεις απόδοσης. Τελευταία βελτίωση αποτελεί η ύπαρξη του παράγοντα χρηστικότητας: μία καθαρή, κατανοητή, προσαρμόσιμη απεικόνιση για το πως η δική μας λύση είναι ζωτικής σημασίας για ταχύτερη ανίχνευση και ευθυγραμμισμένη ανταπόκριση».*

Ανίχνευση. Η αποτελεσματικότητα της πλατφόρμας Kaspersky Anti Targeted Attack Platform έχει ήδη λάβει επαίνους από πελάτες και από ιδρύματα ανεξάρτητων δοκιμών. Η αναβάθμιση του 2017 ενίσχυσε την απόδοση με μεγαλύτερη ενσωμάτωση τερματικών σημείων, μέσω της λύσης ασφάλειας τερματικών σημείων που παρέχεται από την Kaspersky Lab ή ενός αυτόνομου τερματικού σημείου που επιτρέπει στους χρήστες να ανιχνεύουν τις ανωμαλίες στη συμπεριφορά και να αιτούνται περισσότερα δεδομένα για επεξεργασία. Για να επιβεβαιώσουν οι χρήστες ότι ακόμα και μία καλά κρυμμένη επίθεση θα αποκαλυφτεί τελικά, προστέθηκε μία διαδικασία επαναλαμβανόμενου ελέγχου ύποπτων αντικειμένων, τα οποία και αρχειοθετούνται κατευθείαν μόλις προστεθούν.

Αν ένας απειλητικός φορέας φιλοξενεί εξωτερικά ένα κακόβουλο ωφέλιμο φορτίο (όπως συμβαίνει συχνά), η πλατφόρμα Kaspersky Anti Targeted Attack Platform βελτιώνει την ορατότητα και την

ανάλυση μιας επίθεσης. Αυτό επιτυγχάνεται με την επεξεργασία όχι μόνο των αρχείων, αλλά και των διευθύνσεων URL χρησιμοποιώντας ένα sandbox. Ακόμα, είναι πλέον δυνατή η επεξεργασία αρχείων που προστατεύονται με κωδικό πρόσβασης για την αντιμετώπιση μιας άλλης κοινής εγκληματικής τακτικής αποστολής συνημμένων αρχείων προστατευμένων με κωδικό πρόσβασης. Τα αρχειοθετημένα ωφέλιμα φορτία αναλύονται τώρα με ένα καλύτερο ποσοστό ανίχνευσης συνολικά.

Επεκτασιμότητα. Η υποδομή sandbox είναι τώρα αποκεντρωμένη και μπορεί να επεκταθεί ανάλογα με τις ανάγκες ενός πελάτη, με καλύτερη προσαρμοστικότητα στην υπάρχουσα υποδομή (είτε hardware είτε εικονική) και χαμηλότερο κόστος ανάπτυξης. Επιπλέον, η σύνδεση της λύσης με την κυκλοφορία δικτύου και email έχει απλοποιηθεί με πρόσθετες επιλογές ανάπτυξης, κατάλληλες για συγκεκριμένη υποδομή πληροφορικής. Η νέα πλατφόρμα Kaspersky Anti Targeted Attack Platform είναι σε θέση να αποκλείει τα κακόβουλα email όταν ενσωματώνεται στη λύση Kaspersky Security for Mail Gateway.

Ορατότητα. Σήμερα, οι CISOs αντιμετωπίζουν έλλειψη ορατότητας στο κρίσιμο σημείο που καλούνται να λάβουν απόφαση σχετικά με την απόκριση σε περιστατικά. Αποσυνθέτοντας μια αλυσίδα επίθεσης, πρέπει να δουν ολόκληρη την εικόνα και να κατανοήσουν τι είναι πιο σημαντικό να διερευνηθεί – είναι τα δεδομένα του επικεφαλής λογιστή που έχουν τεθεί σε κίνδυνο ή είναι η άδεια BSD στους υπολογιστές Διευθυνόντων Συμβούλων σε περιφερειακά γραφεία; Ένας σημαντικός παράγοντας που βελτιώνει την απόκριση είναι η διαθεσιμότητα ενός ειδικού ασφάλειας που θα παρακολουθεί και θα αναλύει τα αποτελέσματα. Η πλατφόρμα Kaspersky Anti Targeted Attack Platform επιτρέπει αυτό μέσω ενός πλήρως ανανεωμένου πίνακα ελέγχου, με λεπτομερείς πληροφορίες σχετικά με την κατάσταση των περιοδικών ελέγχων, τα πιο πρόσφατα γεγονότα και τις πληροφορίες δεδομένων που έχουν συγκεντρωθεί σε αντίστοιχα γεγονότων. Για να διασφαλιστεί η ιδιωτικότητα, έχουν εφαρμοστεί διαφορετικοί ρόλοι για τους διαχειριστές. Η πρόσβαση σε πληροφορίες σχετικά

με ορισμένα τμήματα της υποδομής με ευαίσθητα δεδομένα μπορεί επίσης να περιοριστεί σύμφωνα με την πολιτική απορρήτου της εταιρείας.

Ο Veniamin Levtsov, Αντιπρόεδρος Enterprise Business της Kaspersky Lab, δήλωσε: «*Τα νέα χαρακτηριστικά της πλατφόρμας Kaspersky Anti Targeted Attack Platform είναι ένα άμεσο αποτέλεσμα των προσπαθειών μας να αντιμετωπίσουμε τα σχόλια των πελατών μας. Μια σειρά αναπτύξεων, συμπεριλαμβανομένης μίας σε ένα σημαντικό χρηματοπιστωτικό ίδρυμα, έδειξε τα πλεονεκτήματα των προηγμένων αλγορίθμων μας, μαζί με την ανάγκη να προσαρμοστούν καλύτερα στις απαιτήσεις των πελατών όσον αφορά την ακρίβεια της ανίχνευσης, την ικανότητα κλιμάκωσης και την ορατότητα.*

Και συνέχισε: «*Καθώς προσαρμοζόμαστε στο συνεχώς μεταβαλλόμενο τοπίο απειλών, είναι σημαντικό να καινοτομούμε, μετατρέποντας την ασφάλεια πληροφοριών σε αποτελεσματικές τεχνολογίες για τους πελάτες μας. Είναι επίσης σημαντικό να βελτιώνουμε συνεχώς τους προηγμένους αλγόριθμους μας και να τους προσφέρουμε με τον τρόπο που επιθυμούν οι πελάτες μας. Εξάλλου, η ευκολία, το κόστος ιδιοκτησίας και η χρηστικότητα συμβάλλουν στην ταχύτερη ανίχνευση και αποκατάσταση των απειλών – όπως κάνουν και οι τελευταίες τεχνολογίες. Καθώς συνεχίζουμε να ενισχύουμε τις δυνατότητες ανίχνευσης και απόκρισης στις λύσεις μας, έχουμε αφιερώσει ένα σημαντικό μερίδιο πόρων για να διασφαλίσουμε ότι τα προϊόντα μας αντανακλούν τις πραγματικές ανάγκες των πελατών μας*».

Περισσότερες πληροφορίες μπορείτε να βρείτε στην επίσημη ιστοσελίδα της εταιρείας.