Από zero-day exploits έως ανεξέλεγκτα “ransomware”: πως εξελίχθηκαν οι προηγμένες στοχευμένες επιθέσεις το δεύτερο τρίμηνο του 2017

Το δεύτερο τρίμηνο του 2017 είδαμε εξελιγμένους απειλητικούς φορείς να εξαπολύουν πληθώρα νέων και βελτιωμένων κακόβουλων εργαλείων, συμπεριλαμβανομένων τριών zero-day exploits και δύο πρωτοφανών επιθέσεων: τις WannaCry και ExPetr. Η ανάλυση των τελευταίων δύο επιθέσεων από τους ειδικούς υποδεικνύει ότι ο κώδικας μπορεί να είχε δραπετεύσει και να κυκλοφορούσε ελεύθερος πριν να είναι πλήρως έτοιμος, μια ασυνήθιστη κατάσταση για επιτιθέμενους που διαθέτουν επαρκείς πόρους. Αυτές και άλλες τάσεις καλύπτονται από την τελευταία τριμηναία αναφορά των ειδικών της Kaspersky Lab.

Από τον Απρίλιο μέχρι και το τέλος Ιουνίου παρατηρήθηκαν σημαντικές εξελίξεις στις στοχευμένες επιθέσεις στη Ρωσία, την Αγγλία, την Κορέα και την Κίνα μεταξύ άλλων. Αυτές οι εξελίξεις έχουν σημαντικές επιπτώσεις στην ασφάλεια των πληροφοριακών συστημάτων των επιχειρήσεων: ανεπτυγμένη κακόβουλη δραστηριότητα συμβαίνει συνεχώς σχεδόν σε όλα τα μήκη και πλάτη του κόσμου, αυξάνοντας το ρίσκο των επιχειρήσεων και των μη κερδοσκοπικών οργανισμών, καθιστώντας τους παράλληλες απώλειες στον ψηφιακό πόλεμο. Οι καταστροφικές επιθέσεις WannaCry και ExPetr – που εικάζεται ότι προκλήθηκαν

από κρατικούς οργανισμούς – στα θύματα των οποίων περιλαμβάνονται αρκετές επιχειρήσεις και οργανισμοί σε ολόκληρο τον κόσμο, ήταν τα πρώτα αλλά κατά πάσα πιθανότητα όχι και τα τελευταία παραδείγματα της νέας επικίνδυνης τάσης.

Στα κυριότερα σημεία του δεύτερου τριμήνου του 2017 περιλαμβάνονται:

- **Τρία zero–day exploits για Windows χρησιμοποιήθηκαν ελεύθερα στο Διαδίκτυο από τους ρωσόφωνους απειλητικούς φορείς Sofacy και Turla**. Το Sofacy, επίσης γνωστό ως APT28 ή FancyBear, ανέπτυξε τα exploits που χρησιμοποιήθηκαν ενάντια σε ένα μεγάλο εύρος Ευρωπαϊκών στόχων, συμπεριλαμβανομένων κρατικών και πολιτικών οργανισμών. Ο απειλητικός παράγοντας παρατηρήθηκε επίσης με τη δοκιμή ορισμένων πειραματικών εργαλείων, κυρίως εναντίον ενός μέλους γαλλικού πολιτικού κόμματος πριν από τις γαλλικές εθνικές εκλογές.
- **Gray Lambert** – Η Kaspersky Lab ανέλυσε το πιο ανεπτυγμένο εργαλείο μέχρι σήμερα για τον όμαδα Lamberts, μία αρκετά εξελιγμένη και περίπλοκη αγγλόφωνη οικογένεια προγραμμάτων ψηφιακής κατασκοπείας. Δύο νέες «συγγενικές» οικογένειες κακόβουλου λογισμικού ταυτοποιήθηκαν.
- **Η επίθεση του WannaCry στις 12 Μαΐου και η επίθεση του ExPetr στις 27 Ιουνίου.** Ενώ είναι πολύ διαφορετικές στη φύση και τους στόχους τους, και οι δύο ήταν εκπληκτικά αναποτελεσματικές ως «ransomware». Για παράδειγμα, στην περίπτωση του WannaCry, η ταχεία παγκόσμια εξάπλωση και το υψηλό προφίλ του έφεραν στο επίκεντρο της προσοχής τη συλλογή Bitcoin από τους επιτιθέμενους, καθιστώντας τη διαδικασία εξαιρετικά δύσκολη. Αυτό υποδηλώνει ότι ο πραγματικός στόχος της επίθεσης WannaCry ήταν η καταστροφή δεδομένων. Οι ειδικοί της Kaspersky Lab ανακάλυψαν περαιτέρω δεσμούς μεταξύ του Lazarus Group και του WannaCry. Το μοτίβο καταστροφικού κακόβουλου λογισμικού μεταμφιεσμένου ως ransomware εμφανίστηκε και

πάλι στην επίθεση ExPetr.

- **Ο ExPetr, με στόχο οργανισμούς στην Ουκρανία, τη Ρωσία και αλλού στην Ευρώπη**, εμφανίστηκε ως ransomware, αλλά αποδείχθηκε καθαρά καταστροφικός. Το κίνητρο πίσω από τις επιθέσεις του ExPetr παραμένει ένα μυστήριο. Οι ειδικοί της Kaspersky Lab έχουν δημιουργήσει μια σύνδεση χαμηλής αξιοπιστίας με τον απειλητικό φορέα γνωστό ως Black Energy.

«Διατηρήσαμε εδώ και καιρό τη σπουδαιότητα της πραγματικά παγκόσμιας Πληροφόρησης απειλών για την ενίσχυση των "υπερασπιστών" των ευαίσθητων και κρίσιμων δικτύων. Συνεχίζουμε να είμαστε μάρτυρες της ανάπτυξης υπεράριθμων επιτιθέμενων χωρίς να λαμβάνουμε υπόψη την «υγεία» του Διαδικτύου και εκείνων που βρίσκονται σε ζωτικά ιδρύματα και επιχειρήσεις που βασίζονται σε αυτό καθημερινά. Καθώς η ψηφιακή κατασκοπεία, η δολιοφθορά και το έγκλημα εξαντλούνται, είναι πολύ σημαντικό για τους "υπερασπιστές" να συσπειρώνονται και να μοιράζονται γνώσεις αιχμής για την καλύτερη προστασία τους από όλες τις απειλές», δήλωσε ο Juan Andres Guerrero-Saade, Παγκόσμια Ομάδα Έρευνας και Ανάλυσης, Kaspersky Lab.

Η έκθεση Q2 APT Trends συνοψίζει τα συμπεράσματα ειδικών εκθέσεων της Kaspersky Lab μόνο για συνδρομητές. Κατά τη διάρκεια του δεύτερου τριμήνου του 2017, η Παγκόσμια Ομάδα Έρευνας και Ανάλυσης της Kaspersky Lab δημιούργησε 23 ιδιωτικές αναφορές για συνδρομητές, με δεδομένα Δεικτών Συμβιβασμού και κανόνες YARA για να βοηθήσουν στη συλλογή εγκληματολογικών στοιχείων και το κυνήγι κακόβουλου λογισμικού.