# Η ESET αναρωτιέται αν οι κυβερνοεγκληματιες της ομάδας TeleBots γίνονται καλύτεροι με την εξάσκηση – PETYA

Η ESET φέρνει στη δημοσιότητα νέα ευρήματα σχετικά με την πιθανή προέλευση των μαζικών κρουσμάτων των παραλλαγών του ransomware Petya.

Σύμφωνα με αποτελέσματα διαχρονικής έρευνας, πολλές από τις εκστρατείες που έχει πραγματοποιήσει η ομάδα κυβερνοεγκληματιών **TeleBots** στην Ουκρανία, καθώς και κάποια στοιχεία από τα διαρκώς μεταβαλλόμενα εργαλεία τους, που έχουν χρησιμοποιηθεί σε επιθέσεις μεταξύ Δεκεμβρίου 2016 και Μαρτίου 2017, εμφανίζουν ομοιότητες με τα κρούσματα του Diskcoder C (γνωστό και ως Petya) που σημειώθηκαν στις 27 Ιουνίου 2017.

«Οι αντιστοιχίες με την επίθεση εναντίον χρηματοπιστωτικών ιδρυμάτων το Δεκέμβριο του 2016, και με την συνακόλουθη ανάπτυξη ενός κακόβουλου λογισμικού KillDisk για Linux που χρησιμοποιήθηκε από την ομάδα TeleBots, αποτελούν ισχυρές ενδείξεις. Αυτές οι ενδείξεις, σε συνδυασμό με τις αυξανόμενες επιθέσεις σε συστήματα υπολογιστών στην Ουκρανία, αξίζουν μιας προσεκτικότερης εξέτασης της ομάδας TeleBots» δήλωσε ο Anton Cherepanov, Senior ESET Malware Researcher.

Ο τρόπος που λειτουργεί η ομάδα TeleBots βασίζεται σταθερά στη

χρήση του KillDisk για να αντικαταστήσει τα αρχεία με συγκεκριμένες επεκτάσεις στους δίσκους των θυμάτων. Δεν υπήρχαν στοιχεία για να επικοινωνήσει το θύμα με τον άνθρωπο που βρισκόταν πίσω από την επίθεση, παρά εμφανιζόταν μία εικόνα από την τηλεοπτική σειρά Mr. Robot. Συνεπώς, ήταν απίθανο να αποσκοπεί σε λύτρα, καθώς τα αρχεία δεν ήταν κρυπτογραφημένα, αλλά είχαν αντικατασταθεί. Ενώ στις επόμενες επιθέσεις προστέθηκε και η κρυπτογράφηση, τα στοιχεία επικοινωνίας και άλλα χαρακτηριστικά του ransomware, τα περιστατικά εξακολουθούσαν να μη συνδέονται.

Από τον Ιανουάριο ως τον Μάρτιο του 2017, η ομάδα TeleBots παραβίασε μια εταιρεία λογισμικού στην Ουκρανία χρησιμοποιώντας VPN tunnels και απέκτησε πρόσβαση στα δίκτυα αρκετών χρηματοπιστωτικών ιδρυμάτων, αποκαλύπτοντας ένα ενισχυμένο οπλοστάσιο εργαλείων σε κώδικα Python. Κατά τα τελευταία στάδια αυτής της εκστρατείας, το ransomware εξαπλώθηκε με τη χρήση κλεμμένων διαπιστευτηρίων των Windows και εργαλείων PsExec της σουίτας SysInternals. Η ESET ανίχνευσε αυτό το νέο ransomware ως Win32/Filecoder.NKH. Ακολούθησε το ransomware για Linux, που ανιχνεύτηκε ως Python/Filecoder.R, το οποίο, όπως μπορεί εύκολα να προβλέψει κανείς, ήταν γραμμένο σε κώδικα Python.

Στη συνέχεια, η ομάδα TeleBots προχώρησε στην εξάπλωση του Win32/Filecoder.AESNI.C (γνωστό ως XData) στις 18 Μαΐου 2017. Διαδόθηκε κυρίως στην Ουκρανία μέσω μιας ενημέρωσης του M.E.Doc, ενός λογισμικού για λογιστική χρήση που χρησιμοποιείται ευρέως στην Ουκρανία. Σύμφωνα με το ESET LiveGrid®, το malware δημιουργήθηκε αμέσως μετά την εκτέλεση του λογισμικού, αποκτώντας τη δυνατότητα αυτόματων πλευρικών κινήσεων μέσα στο παραβιασμένο δίκτυο LAN. Η ESET είχε δημοσιεύσει εργαλείο αποκρυπτογράφησης για το Win32/Filecoder.AESNI.

Ωστόσο, στις 27 Ιουνίου, εμφανίστηκαν μαζικά κρούσματα παραλλαγών του malware Petya (Diskcoder.C) – το οποίο έχει παραβιάσει πολλά συστήματα υποδομών ζωτικής σημασίας και

επιχειρήσεων στην Ουκρανία και παγκοσμίως – με ικανότητα να αντικαθιστούν το Master Boot Record (MBR) με το δικό τους κακόβουλο κώδικα, τον οποίο είχαν δανειστεί από το ransomware Win32/Diskcoder.Petya.

Οι δημιουργοί του Diskcoder.C έχουν τροποποιήσει τον κώδικα MBR έτσι ώστε η ανάκτηση να μην είναι δυνατή, και κατά την εμφάνιση των οδηγιών πληρωμής, όπως γνωρίζουμε πλέον, οι πληροφορίες είναι άχρηστες. Από τεχνική άποψη, υπάρχουν πολλές βελτιώσεις. Ουσιαστικά, μόλις εκτελεστεί το κακόβουλο λογισμικό, προσπαθεί να εξαπλωθεί χρησιμοποιώντας το περίφημο exploit EternalBlue, εκμεταλλευόμενο τη λειτουργία πυρήνα του backdoor DoublePulsar. Πρόκειται για την ίδια ακριβώς μέθοδο που χρησιμοποιείται στο ransomware WannaCry.

Το malware μπορεί επίσης να εξαπλωθεί με τον ίδιο τρόπο όπως το ransomware Win32/Filecoder.AESNI.C (αλλιώς XData), χρησιμοποιώντας μια πιο ελαφριά έκδοση του Mimikatz για να αποκτήσει κωδικούς πρόσβασης και στη συνέχεια να εκτελέσει το κακόβουλο λογισμικό χρησιμοποιώντας τα εργαλεία PsExec της σουίτας SysInternals. Επιπλέον, οι εισβολείς έχουν χρησιμοποιήσει τρίτη μέθοδο για τη διάδοση με τη χρήση μηχανισμού WMI.

Και οι τρείς μέθοδοι έχουν χρησιμοποιηθεί για τη διάδοση κακόβουλου λογισμικού μέσα σε δίκτυα LAN. Όμως, σε αντίθεση με το κακόβουλο λογισμικό WannaCry, στη συγκεκριμένη περίπτωση το exploit EternalBlue χρησιμοποιείται από το Diskcoder.C μόνο σε υπολογιστές μέσα στον εσωτερικό χώρο διευθύνσεων.

Η συσχέτιση της ομάδας TeleBots με αυτή τη δραστηριότητα συνδέεται επίσης με την κατανόηση του λόγου που υπήρξαν κρούσματα και σε άλλες χώρες, εκτός από την συνήθη προσήλωση στην Ουκρανία. Έχουμε καταλήξει στις συνδέσεις VPN μεταξύ των χρηστών του M.E.Doc, των πελατών τους και των συνεργατών τους παγκοσμίως. Επιπρόσθετα, το M.E.Doc διαθέτει ένα εσωτερικό σύστημα ανταλλαγής μηνυμάτων και εγγράφων, οπότε οι επιτιθέμενοι μπορούσαν να στέλνουν μηνύματα spearphishing στα

θύματα. Οι κυβερνοεγκληματίες είχαν επίσης αποκτήσει πρόσβαση στον server που έστελνε τις αυθεντικές ενημερώσεις λογισμικού, την οποία αξιοποίησαν για να στείλουν κακόβουλες ενημερώσεις που εκτελούνταν αυτόματα χωρίς να το έχουν επιλέξει οι χρήστες.

«Έχοντας εισχωρήσει τόσο βαθιά στις υποδομές του M.E.Doc και του πελατολογίου του, οι επιτιθέμενοι είχαν στη διάθεσή τους σημαντικούς πόρους για την εξάπλωση του Diskcoder.C. Παρά την ύπαρξη κάποιων «παράπλευρων απωλειών», η επίθεση έδειξε ότι είχαν βαθιά κατανόηση των πόρων που διέθεταν. Επιπλέον, οι πρόσθετες δυνατότητες του exploit EternalBlue έχουν προσθέσει μια μοναδική διάσταση την οποία θα συναντά όλο και περισσότερο μπροστά της  η κοινότητα του cybersecurity», δήλωσε ο Senior ESET Malware Researcher, Anton Cherepanov.