Ερευνητές ανακάλυψαν πρόσφατα ένα νέο είδος κακόβουλου λογισμικού (malware), το οποίο όχι μόνο προκαλεί σοβαρά προβλήματα σε έναν ηλεκτρονικό υπολογιστή, αλλά στόχος του είναι να τον καταστρέψει ολοσχερώς.

Σύμφωνα με την imerisia το malware, με την ονομασία Rombertik, ανακάλυψαν πρόσφατα οι ερευνητές Μπεν Μπέικερ και Άλεξ Τσίου της Cisco Systems, οι οποίοι δήλωσαν ότι πρόκειται για ένα από τα πιο επικίνδυνα κακόβουλα λογισμικά των τελευταίων ετών. Όπως δήλωσαν οι ερευνητές, το Rombertik έχει σχεδιαστεί για να παρακολουθεί οποιαδήποτε μορφή απλού κειμένου σε έναν browser (πρόγραμμα περιήγησης στο διαδίκτυο) και μεταδίδεται μέσω spam (ανεπιθύμητη αλληλογραφία) ή phishing (ενέργεια για εξαπάτηση χρηστών του Διαδικτύου) μηνυμάτων, αναφέρεται σε έκθεση που ανήρτησε τη Δευτέρα στο μπλογκ της η ερευνητική Ομάδα Talos της Cisco.

Στόχος του συγκεκριμένου malware είναι ηλεκτρονικοί υπολογιστές που ενσωματώνουν το λειτουργικό σύστημα Windows της Microsoft, από όπου αποσπά δεδομένα και πληκτρολογήσεις μέσω phishing. Μόλις εισχωρήσει στο λειτουργικό σύστημα, το Rombertik πραγματοποιεί αλλεπάλληλους ελέγχους προκειμένου να «σιγουρευτεί» ότι δεν έχει εντοπιστεί.

Τέτοιου είδους malware έχουν χρησιμοποιηθεί και στο παρελθόν, όπως στην επίθεση που πραγματοποίησαν πέρυσι χάκερς εναντίον της κινηματογραφικής εταιρείας Sony Pictures Entertainment, για την οποία η κυβέρνηση των ΗΠΑ κατηγόρησε τη Βόρεια Κορέα.

Ο τελευταίος έλεγχος που πραγματοποιεί το Rombertik είναι και ο πιο επικίνδυνος, αναφέρεται στην έκθεση. «Προτού το Rombertik αρχίσει να κατασκοπεύει τα θύματά του, εκτελεί έναν τελευταίο έλεγχο για να βεβαιωθεί ότι δεν έχει εντοπιστεί, ωστόσο εάν καταλάβει κάτι τέτοιο προσπαθεί αυτόματα να καταστρέψει το Master Boot Record (βασική εγγραφή εκκίνησης) προκαλώντας αλλεπάλληλες επανεκκινήσεις στον υπολογιστή και καθιστώντας τον άχρηστο», δήλωσε ο Τσίου. Συνέχισε λέγοντας ότι εάν το malware δεν καταφέρει να «δολοφονήσει» το MBR, τότε προχωρά στην καταστροφή όλων των αρχείων

που βρίσκονται στους κεντρικούς φακέλους του υπολογιστή, κρυπτογραφώντας τους με ένα τυχαίο RC4 κλειδί (αλγόριθμος κρυπτογράφησης).

Μόλις καταφέρει να αχρηστεύσει είτε το MBR είτε τους φακέλους, ο υπολογιστής πραγματοποιεί διαδοχικές επανεκκινήσεις, ενώ στην οθόνη εμφανίζεται το μήνυμα «Carbon crack attempt, failed».

Ο Rombertik στοχοποιεί οποιαδήποτε ιστοσελίδα στον Chrome, τον Firefox ή τον Internet Explorer και εξαπλώνεται μέσω ενός εκτελέσιμου screensaver μεταμφιεσμένο σε αρχείο PDF (Adobe).

Πηγή: techit.gr