Η ESET ανακαλύπτει νέο εξελιγμένο backdoor της ομάδας κυβερνοεγκληματιών Turla

Η ESET έδωσε σήμερα στη δημοσιότητα στοιχεία σχετικά με την ανακάλυψη ενός νέου, προηγμένου backdoor που χρησιμοποιείται από την περιβόητη ομάδα κυβερνοεγκληματιών Turla. Οι ερευνητές της ESET είναι οι πρώτοι που εντοπίζουν αυτό το πρόσφατο backdoor, γνωστό ως Gazer, το οποίο εξελίσσεται διαρκώς από το 2016, στοχεύοντας σε θεσμικά όργανα στην Ευρώπη.

Τυπικά χαρακτηριστικά της ομάδας Turla

Στοχεύοντας σε κυβερνήσεις στην Ευρώπη και πρεσβείες σε όλο τον κόσμο εδώ και πολλά χρόνια, η ομάδα κατασκοπείας Turla είναι γνωστή για τις επιθέσεις τύπου «watering hole» και τις εκστρατείες spearphishing που χρησιμοποιεί στα θύματά της.

Οι ερευνητές της ESET έχουν καταγράψει ότι το Gazer, το backdoor που πρόσφατα ανακαλύφθηκε, έχει μολύνει αρκετούς υπολογιστές σε όλο τον κόσμο, με ένα μεγάλο μέρος των επιθέσεων να έχει στοχεύσει τη νοτιοανατολική Ευρώπη.

«Οι τακτικές, οι τεχνικές και οι διαδικασίες που συναντήσαμε εδώ είναι όμοιες με αυτές που συνήθως βλέπουμε στη δράση της ομάδας Turla», δήλωσε ο Jean-Ian Boutin, Senior Malware Researcher στην ESET. «Αρχικά εγκαταστάθηκε ένα πρώτο

backdoor, δηλαδή το Skipper, πιθανά χρησιμοποιώντας τεχνικές spearphishing, και στη συνέχεια εμφανίστηκε το δεύτερο backdoor στο παραβιασμένο σύστημα, στη συγκεκριμένη περίπτωσή το Gazer.»

Ανιχνεύοντας ένα backdoor που χρησιμοποιεί τεχνικές αποφυγής εντοπισμού

Όπως και τα άλλα εργαλεία που χρησιμοποιεί η ομάδα Turla για να εγκαταστήσει τα δεύτερα backdoor, όπως τα Carbon και Kazuar, το Gazer λαμβάνει κρυπτογραφημένες εντολές από ένα C&C server, που μπορούν να εκτελεστούν είτε σε ήδη μολυσμένο μηχάνημα είτε σε άλλο μηχάνημα στο δίκτυο.

Οι δημιουργοί του Gazer κάνουν επίσης εκτεταμένη χρήση της δικής τους προσαρμοσμένης κρυπτογράφησης, χρησιμοποιώντας τη δική τους βιβλιοθήκη με αλγόριθμους 3DES ή RSA. Τα κλειδιά RSA που βρίσκονται ενσωματωμένα στα backdoor περιέχουν το δημόσιο κλειδί του διακομιστή ελέγχου του εισβολέα και ένα ιδιωτικό κλειδί.

Αυτά τα κλειδιά είναι μοναδικά για κάθε δείγμα και χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που στέλνονται/λαμβάνονται από/προς τον C&C server. Επιπλέον, η περιβόητη ομάδα Turla εμφανίστηκε να χρησιμοποιεί ένα εικονικό σύστημα αρχείων στο μητρώο των Windows για να αποφεύγει τα antivirus και να συνεχίζει να επιτίθεται στο σύστημα.

«Η ομάδα Turla κάνει τα πάντα για να αποφύγει τον εντοπισμό σε ένα σύστημα», συμπληρώνει ο Boutin. «Η ομάδα αρχικά σβήνει αρχεία από παραβιασμένα συστήματα και στη συνέχεια μετασχηματίζει τις συμβολοσειρές και χρησιμοποιώντας διάφορες εκδόσεις backdoor τροποποιεί τα κείμενα σε εφαρμογές με τυχαίο τρόπο.

Σε αυτήν την τελευταία περίπτωση, οι δημιουργοί του Gazer άλλαξαν το κείμενο και εισήγαγαν γραμμές από βιντεοπαιχνίδια όπως «Only single player is allowed». Η ανακάλυψη αυτού του

νέου και αχαρτογράφητου backdoor από την ομάδα ερευνητών της ESET σηματοδοτεί ένα σημαντικό βήμα προς τη σωστή κατεύθυνση για την αντιμετώπιση του αυξανόμενου προβλήματος της κυβερνο-κατασκοπείας στον σημερινό ψηφιακό κόσμο.»

Για περισσότερες τεχνικές λεπτομέρειες σχετικά με το νέο backdoor της ομάδας Turla επισκεφθείτε το σχετικό blogpost ή κατεβάστε ολόκληρο το white paper από το WeLiveSecurity.com.