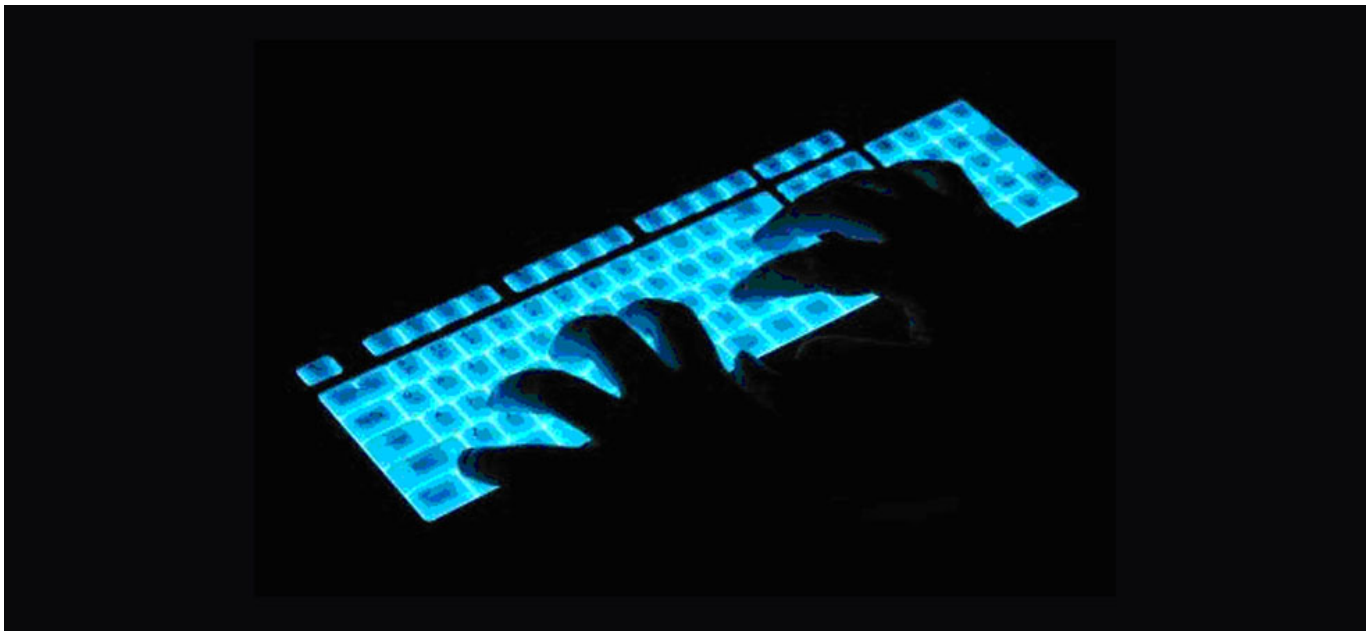
22 Οκτωβρίου 2015

Το Ηνωμένο Βασίλειο δέχεται (κυβερνο) επίθεση

/ Πεμπτουσία

Image not found or type unknown



Οι χρηματοπιστωτικές υπηρεσίες του Ηνωμένου Βασιλείου βρίσκονται υπό την απειλή ενός νέου κύματος επιθέσεων *banking malware* , σύμφωνα με την ερευνητική ομάδα X-Force της IBM.

Η ερευνήτρια cyber security της εταιρείας, *Limor Kessem*, εξηγεί σε ανάρτηση στο ιστολόγιό της ότι η ομάδα της ανακάλυψε μια νέα εκδοχή του *Zeus* που ονομάστηκε *Sphinx:* "Το Sphinx είναι ένα εμπορικό κακόβουλο λογισμικό που θα πωληθεί σε οποιονδήποτε θα πλήρωνε γι' αυτό, κάτι που σημαίνει ότι οι στόχοι του μπορεί να ποικίλουν αρκετά. Η πιο πρόσφατη μορφή του στοχεύει σε διάφορες μεγάλες τράπεζες του Ηνωμένου Βασιλείου αλλά και μία πολωνική τράπεζα. Σε ανάλυση της IBM Security X-Force για το Sphinx, φαίνεται πως ως επί το πλείστον, αποτελεί αντίγραφο των παραλλαγών τ ου Zeus v2. "

Πωλείται για $500 ανα binary, με τον malware author να ισχυρίζεται πως η C&C δομή του μέσω Tor, καθιστά εξαιρετικά δύσκολη την ανίχνευση.

"Το Zeus Sphinx χρησιμοποιείται για την κλοπή online τραπεζικών στοιχείων ταυτότητας, όπως πιστοποιήσεις χρήστη, cookies και πιστοποιητικά. Αυτά τα στοιχεία χρησιμοποιούνται στη συνέχεια από τους απατεώνες σε παράνομες

διαδικτυακές συναλλαγές που συνήθως πραγματοποιούνται από την ίδια τη συσκευή θύματος, ” εξηγεί η Kessem.

“Η σύνδεση με endpoint διευκολύνεται μέσω του backconnect κρυφού virtual network computing (VNC), το οποίο σημαίνει ότι το μολυσμένο endpoint, θα ξεκινήσει μια σύνδεση απομακρυσμένης πρόσβασης στο endpoint του εγκληματία. Αυτό το χαρακτηριστικό επιτρέπει στον εισβολέα να αποκτήσει user-grade πρόσβαση στη συσκευή, ακόμη και μέσα από το firewall. ”

Αυτή τη στιγμή, πάνω από το 50% των στόχων είναι βρετανικές τράπεζες, με τις ΗΠΑ να επηρεάζονται επίσης κατά 38% και την Πολωνία κατά 5%.

Η ομάδα X-Force ανακάλυψε επίσης μια αναβίωση ενός άλλου διάσημου *malware* του περίφημου *Kronos trojan*, που εστιάζει επίσης στις βρετανικές τράπεζες. Ωστόσο, δεν υπάρχουν νέες τεχνικές ενημερώσεις γι’ αυτό το malware, σύμφωνα με τα λεγόμενα της Kessem.

Η ανανεωμένη εστίαση στα χρηματοπιστωτικά ιδρύματα του Ηνωμένου Βασιλείου συμπίπτει με την ανακάλυψη της ομάδας ασφαλείας της IBM αυτή την εβδομάδα, η οποία ισχυρίστηκε ότι το *banking trojan Shifu* είχε “μεταναστεύσει” επιθέσεις από την Ιαπωνία στο Ηνωμένο Βασίλειο.

Η νέα έκρηξη επιθέσεων δεν προκαλεί έκπληξη, δεδομένου ότι το Λονδίνο είναι η οικονομική πρωτεύουσα της Ευρώπης και αποτελεί σημαντικό κομβικό σημείο για την παγκόσμια τραπεζική βιομηχανία.

Πηγή: secnews.gr