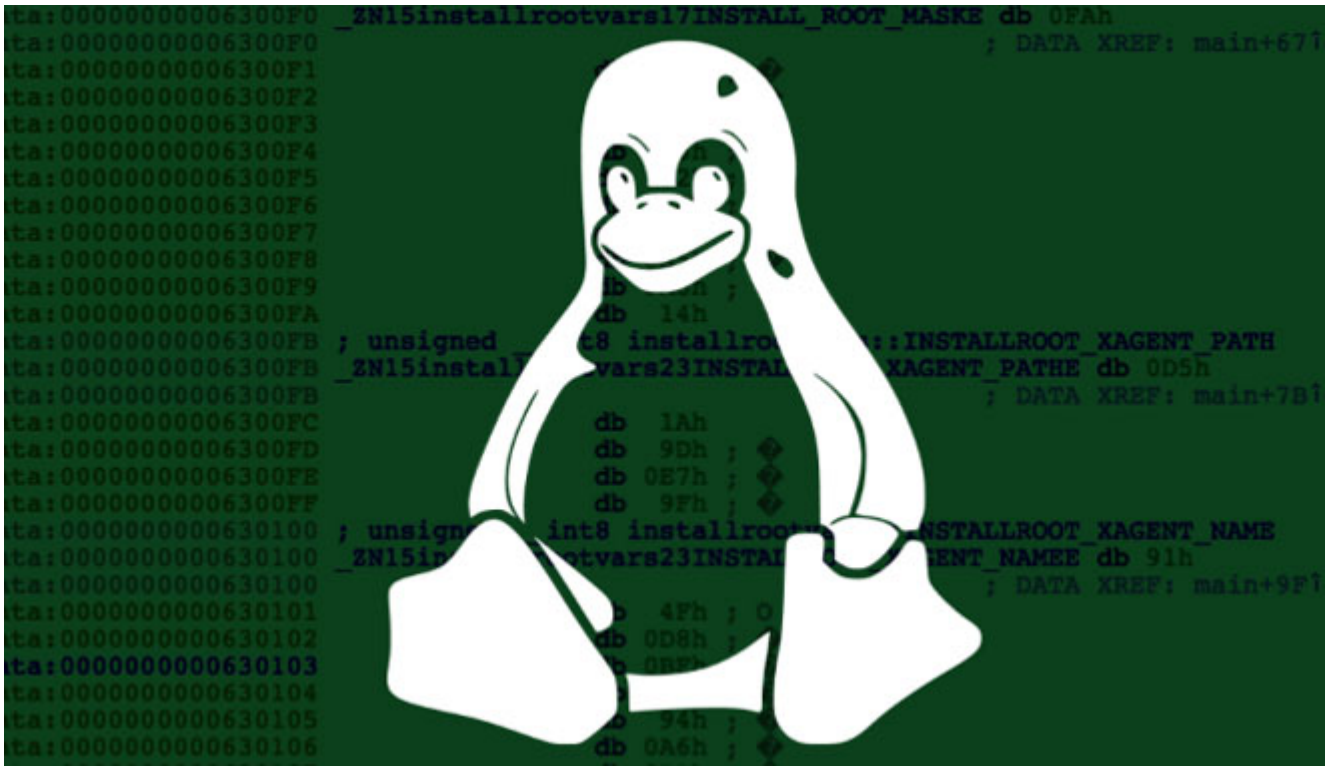
18 Φεβρουαρίου 2016

Fysbis: Ισχυρό όπλο κυβερνοκατασκοπείας στα χέρια Ρώσων hackers

/ Πεμπτουσία

Image not found or type unknown



Το Fysbis συνδέεται με την ομάδα κυβερνο-κατασκοπείας APT 28, η οποία όπως υποστηρίζουν οι ερευνητές έχει την έδρα της στη Ρωσία και διατηρεί πιθανούς συνδέσμους με τις υπηρεσίες πληροφοριών της χώρας.

Το Fysbis (ή αλλιώς Linux.BackDoor.Fysbis) είναι μια πανίσχυρη οικογένεια malware που στοχεύει συστήματα Linux με σκοπό την εγκατάσταση backdoors, επιτρέποντας στους δημιουργούς του κακόβουλου λογισμικού να κατασκοπεύουν τα θύματα και να προβαίνουν σε περαιτέρω επιθέσεις.

Τα πρώτα δείγματα του Fysbis εντοπίστηκαν τον Νοέμβριο του 2014. Ωστόσο, μόλις πρόσφατα, οι ερευνητές ασφαλείας κατόρθωσαν να καταλάβουν πώς λειτουργεί η συγκεκριμένη απειλή και ποιος βρίσκεται πίσω από αυτή.

Βασιζόμενοι στα αποτελέσματα μακροχρόνιας έρευνας, οι εμπειρογνώμονες ασφάλειας της Palo Alto Network κατέληξαν στο συμπέρασμα ότι δεν έχουν να

κάνουν με ένα συνηθισμένο κακόβουλο λογισμικό που μολύνει υπολογιστικά συστήματα αποσκοπώντας στο χρηματικό όφελος, αλλά με μια πολύ πιο εξελιγμένη απειλή που χρησιμοποιείται αποκλειστικά σε εκστρατείες κυβερνο-κατασκοπείας.

Σύμφωνα με τους ερευνητές, το πανίσχυρο αυτό όπλο κυβερνοκατασκοπείας έχει αναπτυχθεί από τη διαβόητη ομάδα hacking APT 28, γνωστή επίσης και ως Sofacy ή Sednit, η οποία δραστηριοποιείται τουλάχιστον από το 2007.

Κατά το παρελθόν, έχουμε αναφερθεί σε αρκετές επιθέσεις της ομάδας, η οποία διατηρεί ρωσικούς δεσμούς και στοχοποιεί κυρίως κυβερνητικούς φορείς, μη-κερδοσκοπικούς οργανισμούς και πολυεθνικές.

Στη λίστα με τους στόχους υψηλού προφίλ της APT περιλαμβάνονται το NATO, το Electronic Frontier Foundation, το ολλανδικό Συμβούλιο Ασφάλειας Αερομεταφορών (Dutch Air Safety Board), η πολωνική κυβέρνηση, καθώς και πλήθος τραπεζών και χρηματοπιστωτικών ιδρυμάτων.

Δεδομένου ότι η ομάδα και οι στόχοι της είναι σε μεγάλο βαθμό ευθυγραμμισμένοι με τα συμφέροντα Κρεμλίνου, αλλά και λόγω της ύπαρξης αρκετών ρωσικών λέξεων στον πηγαίο κώδικα των εργαλείων hacking της APT, οι ερευνητές ασφαλείας είναι πεπεισμένοι ότι συνδέεται άμεσα με τη ρωσική κυβέρνηση, ή τουλάχιστον συνεργάζεται στενά με αυτή.

Πηγή: secnews.gr