27 Μαρτίου 2016

Triada Trojan: το πιο πολύπλοκο mobile malware!

/ Πεμπτουσία

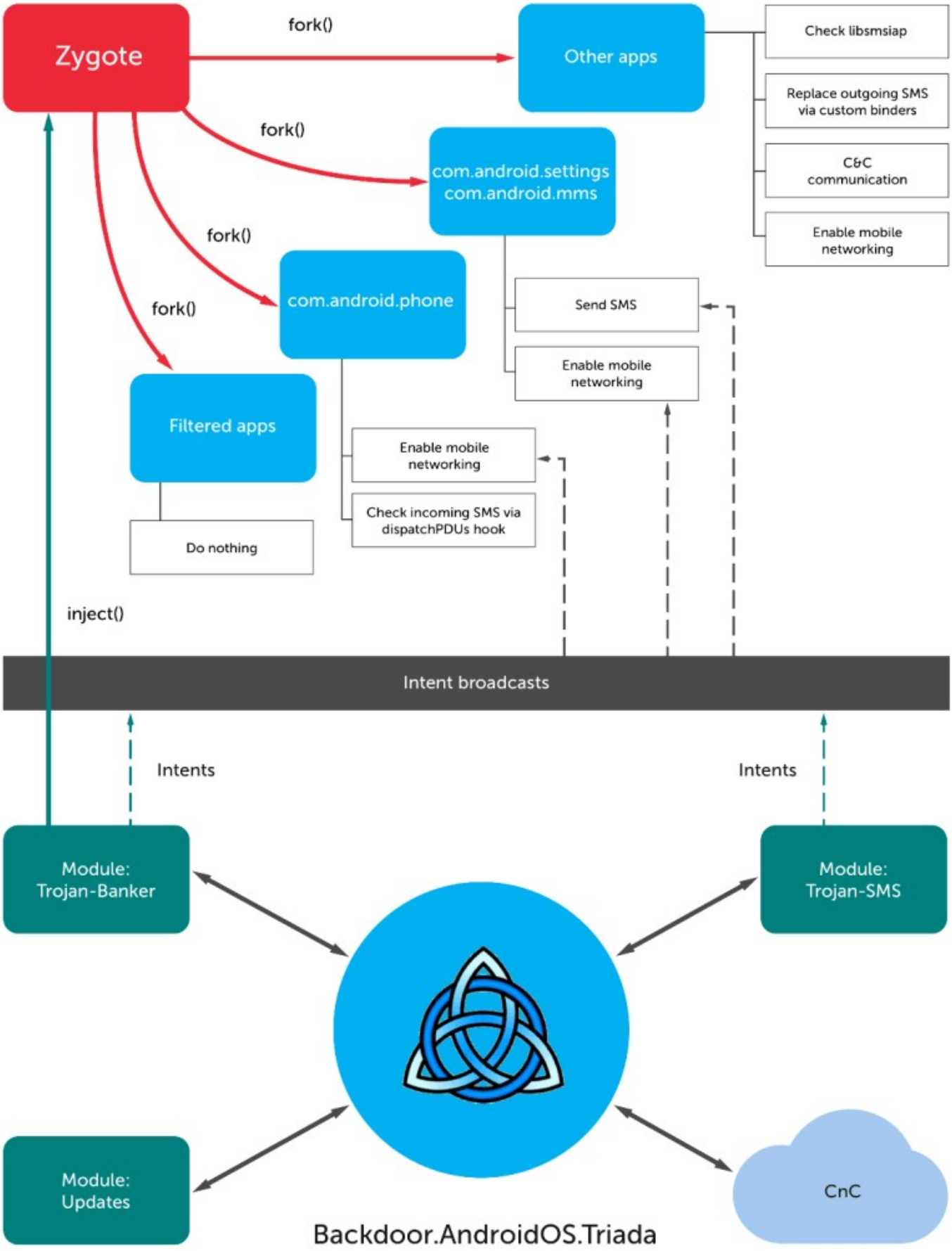
Image not found or type unknown

Η Kaspersky Lab προσφάτως εντόπισε ένα νέο Android malware με την ονομασία Triada Trojan, και το οποίο χαρακτηρίζουν ως το πιο πολύπλοκο κι εξελιγμένο mobile malware που έχουν συναντήσει ως τώρα. !

Οι Malware ερευνητές της Kaspersky Lab ανακάλυψαν ένα νέο strain malware, που ονομάστηκε ***Triada (Backdoor.AndroidOS.Triada)***, στοχεύοντας συσκευές Android, και το οποίο θεωρούν το πιο εξελιγμένο mobile threat που έχουν δει μέχρι σήμερα. Το φάσμα των τεχνικών που χρησιμοποιούνται από την απειλή για να μολύνει mobile devices δεν εφαρμόζονται σε κανένα άλλο γνωστό μέχρι σήμερα mobile malware.

Το Triada σχεδιάστηκε με τη συγκεκριμένη προοπτική και πρόθεση να πραγματοποιεί οικονομικές απάτες, συνήθως hijacking των οικονομικών συναλλαγών μέσω SMS. Το πιο ενδιαφέρον χαρακτηριστικό του Triada Trojan είναι

το modular architecture του, το οποίο του δίνει θεωρητικά ένα ευρύ φάσμα ικανοτήτων.



Το Triada Trojan είναι σε θέση να διεισδύσει σε όλα τα process που τρέχουν στην κινητή συσκευή. Το Android malware διαδίδεται μέσω ενός “advertising botnet” που χρησιμοποιήθηκε από τους απατεώνες για να εξαπλώσουν επίσης και άλλες απειλές, συμπεριλαμβανομένων των Leech, Ztorg και GoPro και του AndroidOS.Iop.

Το Triada Trojan κάνει χρήση της Zygote parent process για την εφαρμογή του κώδικα του στο πλαίσιο όλου του συνόλου των software της συσκευής, πράγμα που ουσιαστικά σημαίνει ότι η απειλή είναι σε θέση να τρέξει σε κάθε εφαρμογή.

Το trojan είναι δύσκολο να ανιχνευθεί, δραστηριοποιείται κυρίως στη μνήμη RAM και εκμεταλλεύεται root privileges για να αντικαταστήσει αρχεία του συστήματος, κρύβει επίσης τα modules του από την λίστα των running/ installed services και applications.

Πηγή: secnews.gr