Viaggio nei malware Android: l'incubo Ransomware

Date : 13 ottobre 2017

(Parte 1)

Introduzione

Il termine **ransomware** suscita ormai panico non solo negli utenti "comuni", ma anche in realtà aziendali dove l'integrità, la confidenzialità e la disponibilità di dati sono essenziali. Per i neofiti di informatica e malware (spesso impropriamente noti come "virus" informatici), con **ransomware** si indica generalmente un malware il cui obiettivo è quello di **criptare** i dati della vittima e di chiedere un **riscatto** al fine di ottenere la chiave utilizzata per decriptare i dati. Nei casi peggiori, la criptazione dei dati si estende anche a tutti i dispositivi USB collegati (inclusi i **backup**) e a tutti i sistemi connessi localmente. I riscatti richiesti variano da centinaia a migliaia di euro, e centinaia di migliaia di varianti di questi attacchi vengono rilasciate ogni anno [1].

Negli ultimi anni, tali attacchi hanno colpito anche gli smartphone, ed in particolare i **dispositivi Android**. Le ragioni di tale fenomeno sono legate, oltre all'enorme diffusione di questo sistema operativo, anche alla natura **open source** di questo, ed alla possibilità di acquistare e scaricare facilmente applicazioni da market di terze parti. Sorge pertanto spontanea la domanda: quali sono le caratteristiche di tali ransomware? Si comportano allo stesso modo delle loro controparti desktop?

La risposta a tale domanda è meno scontata di quanto si possa pensare. Android ha infatti una serie di meccanismi di sicurezza che limitano le operazioni a livello kernel che possono essere eseguite dall'utente: per scrivere ad esempio su aree riservate al sistema operativo, è infatti necessario avere i permessi di **root**, i quali non sono facilmente ottenibili (a meno di effettuare operazioni che possono invalidare la garanzia, quali ad esempio lo sblocco del bootloader). Inoltre, il nuovo modello di permessi introdotto con Android Marshmallow (6.0) consente all'utente di stabilire, durante l'esecuzione dell'applicazione, quali risorse del telefono questa debba utilizzare (in precedenza, i permessi dovevano essere accordati in blocco quando l'applicazione veniva installata).

Di conseguenza, effettuare la criptazione di certi file del sistema operativo Android può non

essere una operazione agevole. Gli attaccanti hanno pertanto capito che, al fine di ottenere un riscatto, non è necessario realizzare una “vera criptazione” di tutti i file, ma è sufficiente bloccare l’utilizzo del telefono. Il tutto cercando di assicurarsi che il ransomware rimanga effettivamente installato nel telefono e resista alla rimozione.

Per questo motivo, i ransomware Android si distinguono in due categorie [1]:

- **Lockers**, ovvero ransomware il cui obiettivo è bloccare l’accesso alla home del telefono e qualunque altra operazione svolta dall’utente.
- **Crypto**, ovvero ransomware che cercano determinati files nella scheda SD, come ad esempio immagini, e le criptano. Per quanto detto sopra, sono in generale “meno distruttivi” delle loro controparti desktop, ma costituiscono comunque un enorme rischio per l’integrità dei dati personali.

Di seguito, andrò a descrivere più in dettaglio le caratteristiche salienti delle due tipologie di ransomware.

Lockers

La caratteristica principale dei lockers è la visualizzazione di una schermata di “blocco” del telefono alla sua accensione, unita alla richiesta di riscatto. In particolare, i lockers adottano delle tecniche di “scaring” (ovvero: spaventare la vittima) che consistono nel mostrare all’utente delle schermate solitamente legate alle forze dell’ordine. Tali schermate spiegano all’utente di aver commesso dei reati, ed illustrano loro la procedura di pagamento del riscatto. La caratteristica più interessante di questi attacchi (i più noti sono **Android/Koler** e **Android/Locker**) è che la schermata cambia nazionalità e tema a seconda della località in cui si trova la persona. Ad esempio, negli Stati Uniti vedremmo una schermata legata all’FBI, mentre in Italia vedremmo la Polizia di Stato, e così via [1,2].

La figura sotto riporta un esempio di varianti “per nazionalità” di Koler (rispettivamente: polizia britannica, polizia svizzera e americana) [3].

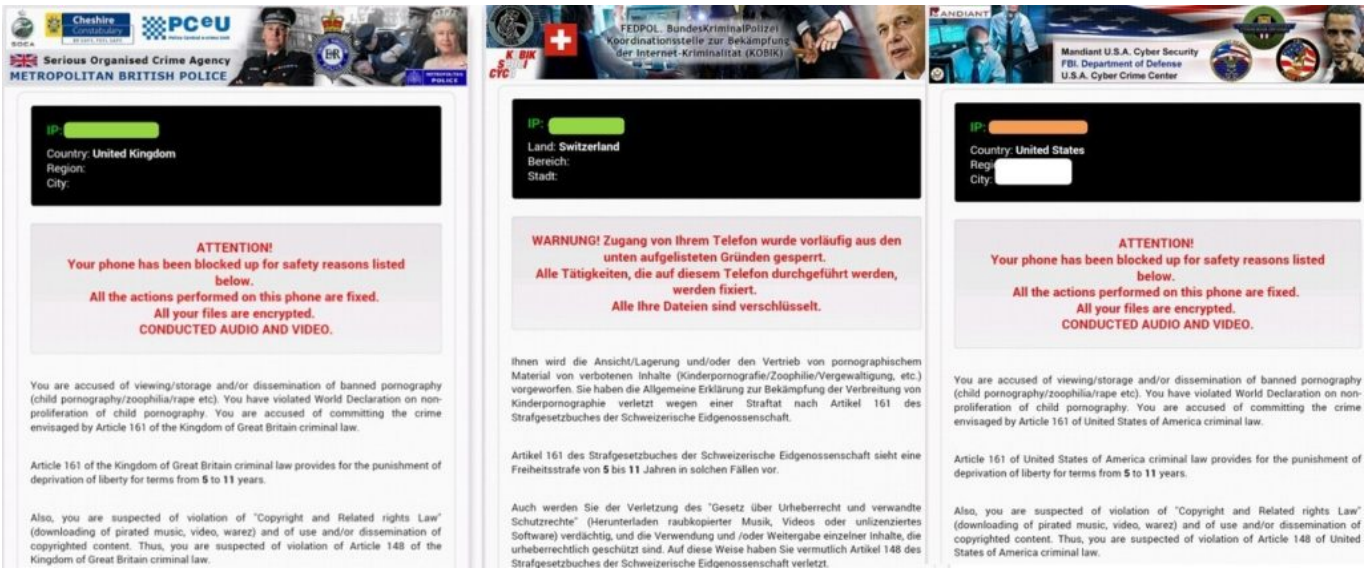

Figura 1 - Esempio di ransomware Koler

Studi scientifici hanno anche portato alla luce la presenza di ransomware di tipo locker provenienti da paesi dell'est Europa. In particolare, la schermata di blocco del dispositivo è rappresentata da una esplicita immagine pornografica accompagnata da scritte in lingua russa [2].

Una variante ancora più pericolosa di locker ransomware prende il nome di **Lockerpin**. Mentre i precedenti ransomware generano la schermata di blocco attraverso un "loop infinito" (cioè la schermata viene richiamata infinite volte, anche se l'utente prova a forzarne la chiusura), i secondi modificano direttamente il pin che consente l'accesso al telefono. Questo è possibile se la vittima accorda i cosiddetti "**Device Administrator Rights**" che, anche se non paragonabili ai permessi di root, consentono ad una applicazione di controllare alcune proprietà del sistema. In questo caso, il processo di rimozione del malware è molto più complesso. Infatti, se la vittima non è più in grado di accedere al telefono, non è nemmeno in grado di usare strumenti come ADB (Android Debugger) dal proprio PC. La soluzione a quel punto diventa, a parte il reset di fabbrica, quella di utilizzare un programma di analisi forense (solitamente, soluzioni molto costose).

L'ultima caratteristica di Lockerpin riguarda la resistenza agli antivirus mobile. Infatti, una volta installato e con i Device Administrator Rights attivati, l'applicazione cercherà tutti i processi legati ad applicazioni antivirus e cercherà di disattivarli o chiuderli.

Crypto-Ransomware

Il principale esponente di questa categoria di Ransomware è **Simplocker.** Il suo obiettivo è quello di criptare determinati files nella scheda SD dell'utente (ad es. .jpg, .pdf, .doc, etc.) presentando, ovviamente, anche la schemata di blocco propria dei Lockers. Una caratteristica interessante di Simplocker è il suo modo di diffondersi. Infatti, spesso questo ransomware si appoggia ad altre applicazioni legittime che semplicemente reindirizzano l'utente al download dell'attacco vero. Questo viene fatto per evitare che i sistemi di analisi automatica del Google Play Store possano bloccare l'applicazione perché malevola [1].

Per spingere l'utente a dare autorizzazioni "indesiderate", questo ransomware adotta una tecnica molto usata da altri malware che si chiama **tap-jacking**. In altre parole, la finestra che richiede i Device Administrative Rights viene "sovrascritta" da un'altra immagine che richiede un semplice aggiornamento. Tuttavia, il bottone con cui si autorizza l'aggiornamento è in realtà riferito all'attivazione dei Device Administrative Rights. In questo modo, il ransomware può immediatamente entrare in funzione.

Altri ransomware (specialmente quelli più vecchi) si presentano come falsi antivirus o come riproduttori di video pornografici.

Le strategie di difesa sono varie, ma si possono riassumere in tre punti fondamentali: 1) Non

scaricare applicazioni di terze parti (disattivare “l’installazione da fonti sconosciute” nelle opzioni Android); 2) Installare un buon anti-malware (la maggior parte sono free); 3) evitare di andare su banner pubblicitari proposti da applicazioni, anche legittime.

Dal prossimo articolo approfondiremo gli aspetti più tecnici del ransomware, andando a descriverne il comportamento “a basso livello”.

References:

[1] ESET. *Trends in Android Ransomware*, Technical Report, 2017.

[2] Davide Maiorca, Francesco Mercaldo, Giorgio Giacinto, Corrado Aaron Visaggio e Fabio Martinelli. *R-PackDroid: Api-Based Characterization and Detection of Mobile Ransomware.* In Proceedings of the ACM Symposium on Applied Computing (SAC), 2017.

[3] Softpedia News. *Koler Android Ransomware Targets Users in 31 Countries*. http://news.softpedia.com/news/Koler-Android-Ransomware-Targets-Users-in-31-Countries-441107.shtml, 2014.

A cura di: **Davide Maiorca**