La Minaccia Mobile e il Mercato Underground

Documento APWG

Figura 1 Nazioni attualmente ad alto rischio di minacce mobili

Scarica il report all'indirizzo www.apwg.org

Italian edition

Responsabile edizione in lingua italiana:
Raoul Chiesa (CLUSIT, APWG)
Contributori:
Selene Giupponi (Security Brokers)
Francesco Mininni (Uff. Esercito Italiano)
Mar CC Riccardo Trifonio (Arma dei Carabinieri)

Con il patrocinio di:

Clusit
Associazione Italiana per la Sicurezza Informatica

Introduzione

Una rapida crescita del mercato della telefonia mobile e una corrispondente diminuzione delle vendite di PC, vedono il 2013 ad un bivio cruciale. Definita nell'analisi di mercato come l'era "post-PC", l'avanzata dei dispositivi mobili presenta un'alternativa interessante, pratica ed economica ai i tradizionali computer desktop. Nei prossimi anni si prevede che i pagamenti effettuati con dispositivi mobili superino la somma di $1.3 trilioni di dollari.

Dal momento che esiste già un mercato consolidato di malware per il mobile, adesso è tempo di bilanci, per dimostrare l'esistenza di una tale "industria sommersa" e come opera attraverso intrusioni abusive e collegamenti con il crimine.

Questo documento descrive questi mercati del malware e dimostra il modus operandi di un'industria che si autofinanzia e che è prospera, verticalmente stratificata e dinamica.

I tipi di malware e i metodi di attacco sotto analisi includono: spyware, attacchi diretti di phishing, trojan, worm, applicazioni trasmesse attraverso malware, botnet portatili (che quindi utilizzano gli smartphone come vettore di contagio e propagazione) ed attacchi combinati, molti dei quali sono fatti apposta per sottrarre somme di denaro agli utenti.

Ugualmente invasive possono essere le tecniche di intrusione "track and trace" usate per carpire informazioni sulle consuetudini e abitudini dei proprietari.

Il report di APWG fornisce dunque un approccio accademico verso il mobile crime e verso la filiera che consente l'intrusione, poiché esamina gli argomenti in profondità dal punto di vista del professionista.

Contenuti

- Minacce Mobili
- Panoramica sull'infrastruttura
- Mercato mobile sommerso
- DNS Mobile e traffico
- iBot e la Botnet mobile
- Intrusioni mobili
- Applicazioni Mobili
- Interventi, Regole e Classificazione
- Guida strategica

Vulnerabilità

- Architettura
- Infrastruttura
- Hardware
- Sistemi di autenticazione
- Software
- Canali di comunicazione/trasporto (Wi-Fi, SMS, Bluetooth)
- Near-Field Communication (NFC)
- Passing the Hash (PtH)

Statistiche e Punti chiave

- Si stima che entro il 2015 ci saranno più di due miliardi di dispositivi mobili.

- La Cina, per esempio, conta adesso 564 milioni di utenti Internet; il 75% sono mobili.
- Sono registrati 5.6 milioni di potenziali file documentati come malevoli su Android (APK, dyn-calls, checks-GPS, etc.), 1.3 milioni dei quali sono confermati come pericolosi da più produttori di AV (Anti Virus).

Esempi di Strumenti e Servizi	Prezzi (US$) - Marzo 2013	Descrizioni esemplificative
Intrusione Mobile (keylogger)	**Open Source - 400**	**Java & Python Keyloggers, Mobistealth,**
Intrusione Mobile (sorveglianza)	**500 – 5,000**	**Finfisher re-ingegnerizzato, Finfisher Lite e copie estese di FlexiSpy**
Malware mobile per frodi bancarie	**10,000 – 30,000**	**Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. potenzialità PtH)**
Botnet Mobili (affitto)	**50 - 400**	**Prezzi all'ora**
Botnet Mobili (operativa e con codice sorgente personalizzato)	**4,000 - 30,000**	**Servizi Mobili di ISP, SMS e mobilità (?? Drive by)**
Malware mobile "black SEO" e programmi di collaborazione occulta	**5,000 – 10,000**	**Usati per redirezionamento del traffico, J2ME midlets, o applicazioni standard per portali popolari.**

Esempi di Strumenti e Servizi	Prezzi (US$) - Marzo 2013	Descrizioni esemplificative
Traffico mobile da nazioni di interesse	**10 – 30 per 1,000 host**	**Può essere acquistato attraverso speciali servizi nell'underground (per area, per nazione)**
Servizi di Spam attraverso SMS	**2-8 cent per 1 SMS**	**Spam Mobile**
Strumenti per lo spam attraverso SMS	**30-50**	**Spam con SMS attraverso klychev v0.3**
Attacchi Mobili con tecniche flooder (Skype o protocollo VoIP SIP)	**30-80**	**Skype Flooder**

Figura 2 – Prezzi attuali del mercato eCrime