Report

Previsioni sulle minacce nel 2012

Di McAfee® Labs™

Indice dei contenuti

Prevedere quali saranno le minacce future può rivelarsi un esercizio approssimativo per un'organizzazione di ricerca in ambito sicurezza. Certamente è interessante indossare il nostro cappello da veggente e pronosticare che cosa accadrà nei prossimi mesi: ma quanto cambiano realmente le minacce di anno in anno? Gli ultimi 12 mesi sono stati un anno di trasformazione sotto molti punti di vista, ma queste trasformazioni sono state rivoluzionarie o di tipo evolutivo? Abbiamo osservato grandi cambiamenti relativamente alle minacce mobile, al fenomeno dell'hacktivism, allo sfruttamento dei client e dei social media e alle minacce mirate. Molti di questi cambiamenti e tendenze continueranno a influenzare il panorama delle minacce negli anni a venire.

Quali cambiamenti per le minacce si aspetta McAfee Labs per i prossimi anni? Prevediamo vari nuovi scenari e alcune evoluzioni significative anche per i vettori delle minacce più affermati:

- Le minacce industriali matureranno e si segmenteranno
- Gli attacchi hardware embedded si estenderanno e si aggraveranno
- Il fenomeno dell'hacktivism e il gruppo Anonymous ripartiranno e evolveranno
- I sistemi di valuta virtuale subiranno attacchi più estesi e frequenti
- Questo sarà "L'anno *per* (non "della") la guerra informatica"
- Le specifiche DNSSEC indirizzeranno nuovi vettori di minacce di rete
- Lo spam tradizionale diventerà "legale," mentre lo spearphishing si trasformerà in un attacco mirato contro i sistemi di messaggistica
- Botnet e rootkit mobile matureranno e convergeranno
- Certificati e enti di certificazione non verificati mineranno la fiducia dei clienti
- I miglioramenti dei sistemi operativi e della sicurezza porteranno a botnet e rootkit di nuova generazione

Lo scenario è delineato, entriamo nei dettagli specifici!

Minacce per il comparto industriale

Le minacce volte a colpire reti di infrastrutture industriali e nazionali hanno di recente attirato l'attenzione e per un ottimo motivo. Questa è una delle poche aree in cui una minaccia cibernetica mette a repentaglio proprietà e vite. I sistemi industriali SCADA (Supervisory Control and Data Acquisition, ovvero controllo di supervisione e acquisizione dati) sono vulnerabili come qualsiasi altro sistema collegato in rete, ma la grande differenza è che molti di questi sistemi non sono stati progettati per l'ambiente di rete che il mondo continua a adottare. La crescente interconnettività di sistemi e dispositivi non progettati per questo tipo di accesso è una ricetta foriera di guai, data la mancanza di pratiche per la sicurezza delle informazioni in molti ambienti in cui i sistemi SCADA vengono implementati. Sembra essere una pratica comune collegare i sistemi d'infrastruttura critici a Internet e poi gestirli con software facilmente reperibile. Tutti i software sono vulnerabili, ma i sistemi IT industriali richiedono una maggior cura e attenzione in termini di architettura, progettazione e implementazione. Gli aggressori sfrutteranno questa mancanza di prontezza con una maggior frequenza e probabilità di successo nel 2012, non fosse altro in termini di e-mail anonime o estorsioni. Quando si esaminano gli obiettivi di molti gruppi di attivisti informatici, il possibile accoppiamento tra obiettivi e programmi politici con le vulnerabilità nei sistemi di controllo industriali (industrial controller systems, ICS) deve essere preso in considerazione *molto* seriamente.

Stuxnet è la dimostrazione che il codice dannoso può dar luogo a una risposta cinetica nel mondo reale[1]. I recenti incidenti indirizzati contro società di fornitura dell'acqua negli Stati Uniti dimostrano che questi impianti sono sempre più obiettivi interessanti per gli aggressori. Maggiore è l'attenzione concentrata sui sistemi SCADA e d'infrastruttura, maggiore è l'insicurezza che sembra venire alla luce. Prevediamo che questa instabilità porterà a minacce maggiori tramite toolkit e framework di exploit e attacchi sempre più frequenti contro sistemi ICS dell'energia e di enti di fornitura di servizi pubblici in particolare. Nel momento in cui un gruppo preso di mira ha dimostrato di avere un punto debole, gli aggressori vi si accaniranno con avidità.

Gli aggressori tendono a ricercare sistemi che possono essere compromessi con successo, e i sistemi ICS hanno dimostrato di essere un ambiente ricco di possibilità d'attacco. I loro amministratori dovrebbero prestare attenzione agli eventi recenti. È giunto il momento di effettuare test di penetrazione approfonditi e pianificare piani di emergenza che includano componenti informatici e networking unitamente all'applicazione delle leggi a tutti i livelli. Devono porsi la seguente domanda: cosa accade quando siamo presi di mira?

La minaccia interna: i sistemi hardware embedded

I sistemi embedded sono cresciuti sia in popolarità che importanza durante gli ultimi anni. In generale, sono progettati per una funzione di controllo specifica all'interno di sistemi di più grandi dimensioni, spesso con requisiti di elaborazione in tempo reale. Spesso risiedono all'interno di un dispositivo completo che include hardware e altre parti meccaniche. Storicamente utilizzata per esigenze industriali in ambito avionica, trasporti e energia e nel settore automobilistico e dei dispositivi medicali, quest'architettura si sta facendo strada sia nel mondo aziendale che in quello consumer. GPS, router, bridge di rete e di recente molti dispositivi di elettronica di consumo utilizzano funzioni e design embedded.

Per sfruttare i sistemi embedded sarà necessario malware che attacca il livello hardware; questo tipo di competenza ha ramificazioni che vanno oltre le piattaforme embedded.

Gli autori di malware ora creano malware che prende di mira i livelli inferiori del sistema operativo sempre più spesso. Molte volte gli aggressori cercheranno di "mettere le radici" in un sistema nel suo livello più basso, incluso il record di boot master e anche i livelli del BIOS. Se gli aggressori possono inserire codice che altera l'ordine di boot o l'ordine di caricamento del sistema operativo, otterranno maggior controllo e potranno mantenere un accesso di lungo periodo al sistema e ai suoi dati.
Il controllo dell'hardware è la terra promessa degli aggressori evoluti.

La conseguenza di questo trend è che altri sistemi che utilizzano hardware embedded saranno suscettibili a questi tipi di attacco. Abbiamo osservato codice di concetto che mira a colpire l'hardware incorporato in sistemi automobilistici, medici e dei servizi di pubblica utilità. Prevediamo che questo codice proofs-of-concept diventerà più efficace nel 2012 e oltre.

Hacktivism

Sebbene il fenomeno dell'hacktivism non sia nuovo, con la saga di WikiLeaks nelle prime pagine di cronaca nel 2010, l'hacktivism ha ottenuto un livello di pubblicità, accettazione e utilizzo più ampio che mai. Nel complesso, il 2011 è stato un anno confuso per gli attivisti online, con protagonisti in conflitto di frequente ai ferri corti l'uno con l'altro e senza obiettivi chiaramente dichiarati. É stato spesso difficile fare chiarezza tra campagne a fine politico e semplici goliardate da parte dei cosiddetti script-kiddie, ma una cosa è risultata lampante: Quando gli attivisti informatici hanno preso di mira un obiettivo, quest'ultimo è stato compromesso o tramite una violazione dei dati o un'interruzione di servizio. Sono una forza credibile. Che si sia d'accordo con i loro obiettivi o meno, Anonymous e altri gruppi di attivisti informatici hanno dimostrato di essere dedicati, pieni di risorse e anche agili nello scegliere obiettivi e operazioni.

Il prossimo anno sarà decisivo per l'hacktivism. E le storie di Anonymous rappresentano solo un aspetto di questo problema.

- Il "vero" gruppo Anonymous (ovvero la sua frangia storica) reinventerà se stesso e l'ambito d'azione oppure si estinguerà. Se i circoli o l'influenza di Anonymous non saranno in grado di organizzarsi - con chiari appelli all'azione e dichiarazioni di responsabilità - tutti coloro che si etichetteranno come Anonymous incorreranno alla fine nel rischio di essere emarginati. In ogni caso, assisteremo a un aumento significativo nel numero di questi attacchi. Gli attacchi DDoS (DIstributed Denial of Service) e la divulgazione di dati personali giustificati da una coscienza politica continueranno a aumentare.
- Coloro a capo delle attività eversive digitali collaboreranno meglio con coloro a capo delle dimostrazioni fisiche. Assisteremo a un maggior accoppiamento dell'hacktivism basato su social media con l'hacktivim coordinato dai social media. Prevediamo che molte operazioni future includeranno componenti sia fisici che digitali. Azioni congiunte e coordinate, sul campo e online, verranno pianificate simultaneamente. Non è difficile prevedere che l'evoluzione di Occupy e altri gruppi oltraggiati includerà azioni online più dirette. Come avevamo affermato in altre previsioni, la possibilità di accoppiare gli obiettivi degli attivisti informatici con la disponibilità dei sistemi di controllo industriali o dei sistemi SCADA è una possibilità molto reale. Prevediamo che gli attivisti informatici più estremisti che supportano i movimenti Occupy a livello mondiale abbandoneranno l'etichetta Anonymous e presto opereranno con il nome di "Cyberoccupiers".
- Le vite private di personaggi pubblici - politici, leader di settore, giudici e responsabili della sicurezza e delle forze dell'ordine - saranno rese pubbliche quest'anno molto più che in passato per fini politici e ideologici. I contestatori non si fermeranno davanti a niente per ottenere i dati dai social network o dai server web per supportare le loro diverse operazioni.

- Alcuni attivisti informatici opereranno sulle stesse linee dei vari "eserciti cibernetici" che fioriscono principalmente in stati non democratici o non laici (Iranian Cyber Army, Pakistan Cyber Army, gruppo ChinaHonker, ecc.). Utilizzati in larga parte per attacchi di defacciamento negli ultimi due anni, gli eserciti passeranno a azioni più dirompenti nel nuovo anno. Alcuni di questi gruppi si scontreranno tra di loro, causando probabilmente danni collaterali non prevedibili (Palestinesi contro Israele, Indiani contro Pakistani, Corea del Nord contro Corea del Sud, ecc.) Nel 2011, correva voce che gli eserciti cibernetici erano manipolati o supportati dai loro governi. Il prossimo anno, gli stati totalitari faranno un passo avanti, riconoscendo addirittura le azioni degli eserciti cibernetici locali.

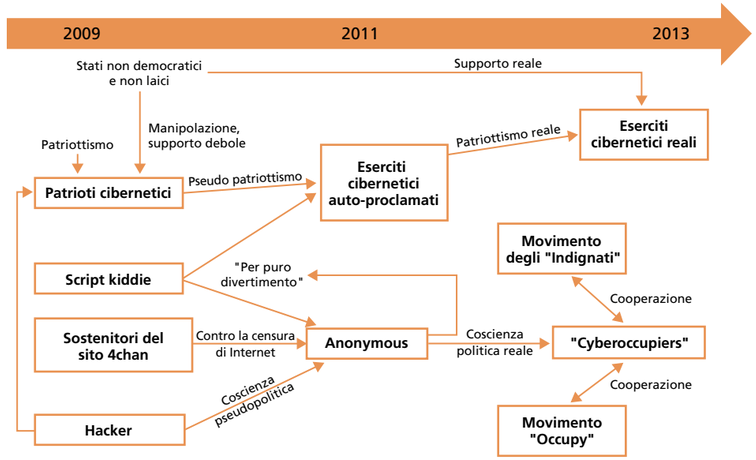

Figura 1. Le molte connessioni e motivazioni dell'hacktivism.

Valuta virtuale

La valuta virtuale, alcune volte denominata valuta cibernetica o cybercurrency, è diventata un modo diffuso per la gente per scambiare denaro online. Sebbene non necessariamente sostenuti da risorse to addirittura merci tangibili, servizi come Bitcoin permettono agli utenti di effettuare transazioni attraverso una rete pee-to-peer decentralizzata; essenzialmente denaro elettronico che permette di effettuare pagamenti online diretti. Un utente necessita solo di un software client e di un servizio di pagamento online (wallet) per ricevere il "denaro", che viene conservato nel wallet e può essere trasferito ad altri come pagamento di beni o servizi. Per inviare e ricevere tale denaro, gli utenti hanno semplicemente bisogno dell'indirizzo del wallet. Riuscite a cogliere sia il problema che l'opportunità?

Il malware trojan ben si adatta a questa architettura. I wallet non sono cifrati e le transazioni sono pubbliche. Ciò li rende un obiettivo allettante per i criminali informatici. Vari eventi degni di nota si sono verificati nel 2011 relativamente alle valute virtuali:

- Il database di scambio di Bitcoin Mt. Gox è stato preso di mira da aggressori che hanno rubato migliaia di Bitcoins (soldi digitali)
- Era stato distribuito spam che promuoveva falsi strumenti di mining Bitcoin. Questi strumenti in realtà contenevano malware studiato per inviare i file relativi ai wallet delle vittime a una postazione remota. Permettevano inoltre a altri pirati informatici di utilizzare il computer infettato per attaccare ulteriormente Bitcoin.
- Le botnet di Bitcoin sono state riscontrate "in the wild". Utilizzando un gran numero di macchine infette, queste botnet potrebbero velocizzare gli attacchi di mining ed elaborazione Bitcoin e potrebbero anche lanciare attacchi DDoS.

La natura delle valute e delle tecnologie virtuali come Bitcoin sono un obiettivo troppo allettante perché i criminali cibernetici lo ignorino. Nel 2011, abbiamo osservato una crescita considerevole del malware rivolto contro queste tecnologie. Diamo uno sguardo al malware Bitcoin, in particolare:

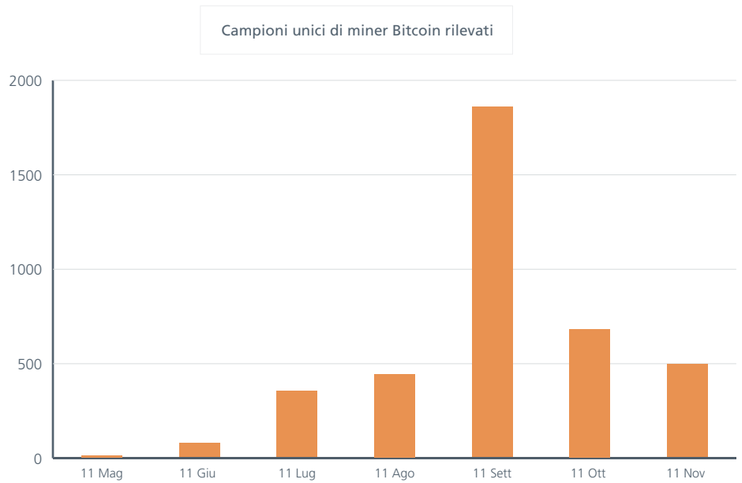

Figura 2. Il furto (chiamato "mining") della valuta virtuale Bitcoin ha raggiunto un picco in Settembre. Prevediamo che i furti aumenteranno nel 2012.

Prevediamo che il prossimo anno questa minaccia si trasformerà in un lavoro a domicilio del crimine informatico, laddove spam, furto di dati, strumenti, reti di supporto e altri servizi associati dedicati esclusivamente a sfruttare le valute virtuali. Chiaramente, i criminali cibernetici hanno fondato un sistema di pagamento che soddisfa le loro esigenze.

Guerra informatica

Sarà questo l'anno della guerra informatica, o semplicemente una dimostrazione di armi cibernetiche offensive e del loro potenziale? Sebbene ovviamente speriamo si tratti della seconda ipotesi, il montare della situazione negli ultimi anni rende un'eventuale guerra informatica pressoché inevitabile. Abbiamo osservato di frequente tecniche "cibernetiche" a completamento di tradizionali metodi di intelligence o spionaggio, con molti protagonisti che accusano altri, amici e avversari. Si tratta di un modo economico di spiare, che lascia sempre spazio per negare tutto in modo plausibile, non mette in pericolo vite umane e, fondamentale, sembra essere estremamente efficace. Invece, non è così diffuso l'utilizzo della "cibernetica" come parte dell'arsenale a disposizione in un conflitto armato. Al momento, questo fenomeno è stato rilevato solo su piccola scala con un livello di sofisticazione degli attacchi molto limitato, per esempio, nel conflitto in Georgia.

Ma la situazione è cambiata. Molte nazioni si rendono conto del potenziale invalidante degli attacchi informatici contro le infrastrutture critiche e quanto è difficile proteggersi di conseguenza. Il loro potenziale apre a possibilità di attacco da parte di piccole nazioni o organizzazioni, in particolare se c'è un numero limitato di obiettivi contro cui reagire. L'attacco Stuxnet è stato un attacco rivoluzionario per molti aspetti, uno dei quali è il fatto che ha chiarito a tutti che la minaccia è reale e l'impatto che tali attacchi potrebbero avere.

Gli Stati Uniti si sono resi conto di quanto sono vulnerabili, probabilmente più di ogni altra nazione data la loro incredibile dipendenza dai sistemi informatici e da una difesa informatica che fondamentalmente protegge solo le reti governative e militari (immaginiamo un esercito che protegge solo le basi militari invece che ogni altra parte della nazione). Dopo aver raccolto diverse critiche per l'assenza di una dottrina formale, la nazione ha finalmente reagito.

A luglio è stata rilasciata la "Department of Defense Strategy for Operating in Cyberspace" (Strategia del Dipartimento della Difesa per le operazioni nel ciberspazio)[2]. Il report afferma (NdT: traduzione libera) "Strategic Iniziativa strategia 1: Il Dipartimento della Difesa (DoD) tratterà il ciberspazio come un dominio operativo da organizzare, formare e equipaggiare in modo da poter sfruttare appieno il potenziale del ciberspazio". Ma in questo documento non è presente un argomento di cui abbiamo discusso in precedenza, ovvero che gli attacchi cibernetici di sufficiente impatto potrebbero portare a contrattacco. Invece, il DoD sta preparando una nuova dottrina per completare la strategia per il ciberspazio che offra linee guida concrete per il proprio staff dedicato alla guerra informatica. Se tale dottrina delinea in quali circostanze dovrebbe essere presa in considerazione una ritorsione cibernetica, saremmo ancora lontani da quella dottrina della "minaccia di annientamento totale" che ha aiutato il mondo a sopravvivere alla guerra fredda.

In realtà, se la possibile reazione non è nota perché è segreta, non è in grado di dissuadere nessuno dallo sferrare un attacco.

Secondo vari report, durante la rivoluzione in Libia era stato preso in considerazione l'utilizzo delle armi cibernetiche ma ciò non si è poi verificato perché nessuno voleva essere il primo ad aprire il vaso di Pandora. O, forse, semplicemente non era un ambiente ricco di obiettivi. Per il momento, tuttavia, non abbiamo assistito ad alcuna dimostrazione pubblica delle possibilità di offensiva della guerra informatica che abbiano il potenziale di dissuadere qualcuno. Saranno sempre più pressanti le richieste per togliere il segreto di stato da tali informazioni, perciò ci aspettiamo una qualche forma di dimostrazione, diversa dal mostrare ai diplomatici stranieri video allarmanti di mancanza di mezzi. Una dimostrazione efficace ha il potere di scatenare una risposta del tipo "anche io" da parte di altri stati, per dimostrare che dispongono delle stesse possibilità.

Per gli anni a venire ci auguriamo di assistere solo a dimostrazioni, piuttosto che a qualche effetto di una guerra informatica reale!

DNSSEC

Il protocollo DNSSEC (Domain Name System Security Extensions, Estensioni per la sicurezza del DNS) protegge i servizi di name-resolution da raggiri e "avvelenamento" della memoria cache utilizzando un "web di fiducia" basato sulla cifratura a chiave pubblica. È volto a impedire che un computer client comunichi inavvertitamente con un host a seguito di un attacco man-in-the-middle, che reindirizza il traffico dal server voluto (pagina web, e-mail, ecc.) verso un altro server. Proteggere gli utenti online e approntare un terreno più difficoltoso per gli hacker rappresenta un importante passo avanti nell'evoluzione di Internet.

Sfortunatamente il DNSSEC protegge anche contro i raggiri e il reindirizzamento dei tentativi da parte delle autorità che cercano di reinstradare il traffico verso siti web che trafficano in software o immagini illegali. Affinché un governo possa reindirizzare il traffico, dovrebbe essere considerato autorevole dai domini a livello di root, che è un livello di fiducia che altri enti governativi esiterebbero a garantire se sapessero che il risultato sarebbe la soppressione dei contenuti Internet sulla base di opinioni di governi stranieri.

I recenti tentativi di legiferare per prevenire l'erogazione di proprietà intellettuale si basano sulla comprensione dello stato attuale di come il sistema DNS opera attualmente e non su come opererà il DNSSEC futuro. Questo divario potrebbe creare la necessità di ulteriori requisiti legati per gestire l'attuale infrastruttura DNS, che potrebbe non essere compatibile con l'infrastruttura DNSSEC. Se vengono implementati tali requisiti, allora il processo per il miglioramento della sicurezza della nostra infrastruttura DNS potrebbe essere sospeso mentre i comitati cercano un terreno tecnico comune tra la legge e il DNSSEC.

Gli enti governativi di tutto il mondo si stanno sempre più interessando a stabilire "regole della strada" per il traffico Internet, perciò possiamo prevedere di assistere un numero sempre maggiore di casi in cui le soluzioni di domani vengono ostacolate da dispute legislative relative ai problemi di ieri. Il risultato: l'Internet di domani probabilmente assomiglierà a quella di ieri per un periodo superiore a quello che noi, seguaci della sicurezza, vorremmo vedere.

Lo spam "legittimo"

Negli ultimi quattro anni abbiamo assistito all'aumento di consapevolezza e cooperazione a livello internazionale per combattere lo spam correlato alle botnet. Tale collaborazione è risultata nella chiusura di varie infrastrutture di alto profilo che erano fondamentali per il controllo delle botnet (come il provider McColo), per l'hosting dei domini di spam (Glavmed) e per l'elaborazione di carte di credito legata ai farmaci contraffatti. È stata efficace anche contro grandi imprese Internet che fornivano spazi pubblicitari a società illecite. Queste azioni hanno portato a una drastica diminuzione dei volumi globali di spam, dopo il picco di metà 2009, e hanno aumentato significativamente i costi sommersi dell'invio di spam tramite botnet.

Anche se questi risultati non rappresentano assolutamente la fine dello spam, come hanno predetto alcuni guru della tecnologia, contribuiscono a cambiare il panorama. Oggi vediamo infatti sempre di più che lo spam indesiderato non parte da host infettati da botnet ma da agenzie pubblicitarie "legittime", utilizzanti tecniche fortemente deplorate dalla comunità antispam. Queste azioni comportano l'inclusione di indirizzi e-mail, senza che gli utenti abbiano dato il consenso o siano stati avvisati, in elenchi dalla finalità pubblicitaria. Le tecniche usate sono varie: l'acquisto sfrontato di elenchi di indirizzi e-mail, pubblicizzati come provenienti da utenti che hanno dato il loro consenso alla ricezione di materiale pubblicitario (affermazione che richiede una decisa sospensione dell'incredulità), l'"e-pending" (raccolta di indirizzi e-mail tramite algoritmi che decidono quali persone direbbero sì all'invio di pubblicità se gli fosse chiesto, poi saltano la domanda e li aggiungono agli elenchi senza autorizzazione), l'acquisto di database di clienti di aziende fallite e che evidentemente ignoravano il diritto alla privacy quando erano in attività, fino al "partenariato" con altre entità pubblicitarie o fornitori di mailing list per imbottire di pubblicità i loro elenchi di indirizzi.

Le compagnie pubblicitarie che si comportano in questo modo sono consapevoli di inviare spam e usano le stesse tecniche impiegate dagli operatori botnet per eludere il rilevamento. Ogni giorno migliaia di nuovi domini di posta elettronica vengono registrati con il protocollo di privacy whois per impedire l'identificazione del proprietario, mentre migliaia di nuovi indirizzi IP vengono attivati nelle sottoreti dei provider di hosting per poche ore, al fine di inviare una raffica di spam che intasa le caselle di posta con e-mail malformattate e piene di errori grammaticali e sintattici. La maggior parte di queste e-mail contengono un link che apparentemente permette di poter essere esclusi dagli invii, mentre invece l'unica cosa che fa è di rendere noto allo spammer che l'indirizzo di posta elettronica è attivo e che l'utente sta leggendo il messaggio. È presente anche un indirizzo postale cui mandare una lettera per chiedere di venire tolti dagli elenchi, ma cercando l'indirizzo in rete si scopre che corrisponde magari alle foreste canadesi o a un appezzamento di terreno nel deserto dell'Arizona. In certi casi, singoli indirizzi e-mail hanno ricevuto oltre 9000 messaggi di spam identici in un solo giorno, che pubblicizzavano i vantaggi per la salute di un braccialetto magnetico di moda.

Queste pratiche pubblicitarie disoneste sono poi supportate dalla legge. La legge statunitense CAN-SPAM è stata così tanto alleggerita che non è necessario ricevere il consenso dei destinatari per l'invio di materiale pubblicitario. Dato che la pubblicità è un'attività molto redditizia e gode di una forte attività di lobby, a breve termine sono molto improbabili dei cambiamenti significativi alle pratiche di gestione degli elenchi di e-mail o anche multe salate per i comportamenti scorretti.

In questo contesto possiamo attenderci di vedere l'aumento dello spam "legale" a un tasso allarmante. Inviare spam agli individui tramite agenzie pubblicitarie è meno costoso e meno rischioso che tramite host infettati dalle botnet. Questo tipo di attività, noto come "snowshoe spamming", è aumentato così tanto che al momento di redigere questo articolo tra i 10 oggetti più comuni delle e-mail ve ne erano uno relativo alla "notifica dello stato di consegna", uno correlato allo spam botnet dei finti Rolex, uno alla "confidence scam" e ben sette associati allo snowshoe spam. Questo genere di traffico continuerà ad aumentare a un tasso superiore a quello del phishing e delle truffe basate sulla fiducia, mentre lo spam correlato alle botnet continuerà a diminuire in quanto i proprietari delle bot trovano modi sempre migliori e più sicuri per estorcere denaro dai loro eserciti di computer infetti. È solo una questione di tempo prima che la maggior parte del volume globale di spam provenga da entità che si comportano scorrettamente ma che sono "legali".

Minacce mobile

Negli ultimi due anni abbiamo assistito a un aumento degli attacchi verso smartphone e dispositivi mobili. Ci siamo imbattuti in rootkit, botnet e altro malware. Gli aggressori si sono spostati dal malware semplicemente distruttivo allo spyware e al malware che generano soldi. Li abbiamo visti sfruttare le vulnerabilità per eludere le protezioni dei sistemi e ottenere un maggiore controllo sui dispositivi mobili. Nel 2012 ci aspettiamo che gli aggressori continuino su questa strada e anzi migliorino i loro attacchi. Prevediamo inoltre uno spostamento verso gli attacchi al banking mobile.

Botnet + rootkit = problemi di basso livello

Nei PC i rootkit e le botnet inviano pubblicità per spillare soldi alle proprie vittime. Sui dispositivi mobili abbiamo osservato questi tipi di malware usati nello stesso modo. I rootkit consentono l'installazione di software aggiuntivo o di spyware, mentre le botnet possono portare a clic sulla pubblicità o l'invio di messaggi SMS a tariffe maggiorate.

Abbiamo visto varianti di famiglie di malware, fra le quali Android/DrdDream, Android/DrdDreamLite e Android/Geinimi, oltre che Android/Toplank e Android/DroidKungFu. Alcuni di questi malware hanno usato le vulnerabilità root, sviluppate originariamente per consentire lo sblocco dei telefonini, al fine di accedere ai cellulari delle vittime e di impadronirsene. Nel prossimo anno, mentre sviluppatori e ricercatori creeranno nuovi metodi per il rooting dei telefoni, vedremo gli autori di malware applicare le lezioni apprese in termini di malware PC per sferrare su più ampia scala gli attacchi che sfruttano il livello hardware dei dispositivi mobili. Il malware basato su PC sta scavando sempre di più nel sistema operativo (SO) al fine di sfruttare ancora di più l'hardware; ci aspettiamo che il malware mobile vada nella stessa direzione.

Anche i bootkit, malware che sostituisce o bypassa l'avvio del sistema, minacciano i dispositivi mobili. Anche se eseguire il rooting del proprio telefonino o lettore di ebook apre il dispositivo a funzioni aggiuntive o alla sostituzione del sistema operativo, può permettere anche agli aggressori di caricare il proprio sistema modificato. Mentre un rootkit mobile modificherà semplicemente il sistema operativo esistente per eludere il rilevamento, un bootkit può assegnare a un aggressore un controllo molto superiore di un dispositivo.

Per esempio, il toolkit per i test di penetrazione sui dispositivi mobili chiamato "Weapon of Mass Destruction" (Arma di distruzione di massa) gira sui vecchi cellulari con Windows Mobile. Il WMD si installa tramite gli strumenti sviluppati per caricare Linux sui cellulari Windows Mobile e consente all'utente di riavviare il sistema operativo originale. Gli aggressori hanno già usato vecchi exploit root per nascondersi; con lo sviluppo di nuovi exploit gli aggressori giungeranno a installare il proprio firmware personalizzato.

Gli attacchi al banking mobile

Gli utenti dei PC hanno osservato attacchi provenienti da criminali che utilizzano i kit di crimeware Zeus e SpyEye per sottrarre denaro dagli account di banking online. Sia Zeus che SpyEye hanno iniziato a usare le applicazioni mobili per eludere l'autenticazione a due fattori e avere accesso al denaro delle vittime.

Zitmo (Zeus-in-the-mobile) e Spitmo (SpyEye-in-the-mobile) sono due famiglie di spyware mobile che inoltrano messaggi SMS agli aggressori. L'utilizzo di questo spyware richiedeva agli aggressori l'accesso manuale per poter rubare denaro agli utenti.

Nel luglio scorso, il ricercatore sulla sicurezza Ryan Sherstobitoff ha spiegato il modo in cui le transazioni eseguite dai criminali che usano Zeus e SpyEye potrebbero essere tracciate, dato che sono del tutto dissimili da quelle degli utenti legittimi. Il mese scorso ha mostrato come i criminali si sono adattati per rapinare in modo programmatico le proprie vittime mentre queste sono ancora nei propri account. In tal modo le transazioni illecite sembrano provenire dagli utenti legittimi e con l'aggiunta di un ritardo appaiono come eseguite da un umano. Gli aggressori si sono adattati rapidamente a ogni cambiamento mirato a proteggere il banking nei PC. Dato che usiamo i dispositivi mobili sempre di più per effettuare operazioni bancarie, osserveremo gli aggressori scavalcare i PC e mirare direttamente alle applicazioni di banking mobile. Ci aspettiamo di vedere con sempre maggiore frequenza gli attacchi che sfruttano questo tipo di tecniche di programmazione, dato che sempre più utenti gestiscono le proprie finanze sui dispositivi mobili.

I certificati fraudolenti

Tendiamo a fidarci di file e documenti quando sono dotati di firma digitale, grazie alla fiducia riposta nelle firme e nelle autorità di certificazione da cui provengono. Molti sistemi di whitelisting e per il controllo delle applicazioni dipendono da firme digitali valide. Queste soluzioni ci consentono di porre in essere policy e controlli per servizi, applicazioni e persino file che rechino una firma digitale valida. Anche la navigazione web e le transazioni online sicure si affidano alle firme digitali attendibili. In pratica, queste autorità di certificazione e i loro certificati dicono al sistema operativo: "Puoi fidarti di me perché sono valido e garantito".

Data questa fiducia, cosa succede quando ci capita un certificato digitale illecito o falso? Per approfondire, quali sono le implicazioni di un'autorità di certificazione compromessa? I certificati digitali ci consentono un certo livello di fiducia in un file, un processo o una transazione. Producendo e mettendo in circolazione certificati falsi o illeciti, gli aggressori possono sferrare attacchi praticamente invisibili. Nel browser ciò consente a un aggressore di avviare attacchi di tipo "man in the middle": il traffico normalmente criptato e non visualizzabile da parte dell'aggressore diventa ora chiaro e leggibile perché questi possiede la "chiave". Nell'host, il software di sicurezza ignorerà un file firmato con una chiave valida in quanto risulterà incluso in una white list: sarà autorizzato all'accesso grazie al certificato che presenta.

Minacce recenti quali Stuxnet e Duqu hanno usato certificati illeciti con grande successo per eludere il rilevamento. Anche se non è la prima volta che osserviamo questo comportamento (i certificati illeciti sono stati usati dagli antivirus fasulli, da certe varianti di Zeus e Conficker e anche da qualche vecchio malware Symbian), ci attendiamo un aumento di questa tendenza nel 2012 e oltre.

L'accresciuta minaccia consistente nel prendere di mira le autorità di certificazione per produrre certificati illeciti è una preoccupazione per il futuro, anche perché questo tipo di compromissione consentirebbe a un aggressore di creare chiavi multiple utilizzabili in diversi scenari basati su web e su host, minando effettivamente gran parte della fiducia riposta in un sistema operativo. Siamo molto preoccupati delle implicazioni dovute all'uso su vasta scala dei certificati illeciti, relativamente al whitelisting e alle tecnologie di controllo delle applicazioni che usano tali certificati. DigiNotar, un'autorità olandese già travagliata, ha di recente dichiarato bancarotta dopo una violazione della protezione che ha prodotto l'emissione di certificati fraudolenti. Quest'attacco è stato il colpo di grazia? Le indagini hanno rivelato che DigiNotar ne aveva emessi ben 531. È probabile che, analizzando più a fondo le violazioni in questo settore, il fallimento di questa società non sia un caso isolato. Ora dobbiamo preoccuparci dei danni prodotti e della perdita di fiducia.

Gli attacchi su vasta scala alle autorità di certificazione e il più ampio uso di certificati digitali validi, ma fraudolenti, si estendono all'infrastruttura delle chiavi pubbliche, alla navigazione protetta e alle transazioni, oltre che alle tecnologie basate su host come il whitelisting e il controllo delle applicazioni. Lo sfruttamento della fiducia in questo sistema dà agli aggressori un grande vantaggio, perciò si concentreranno sicuramente in quest'area.

I progressi nei sistemi operativi

La sicurezza delle informazioni comporta un continuo testa a testa, a ogni azione corrisponde una contromisura. Gli aggressori scrivono del codice malevolo, noi lo contrastiamo. I produttori di sistemi operativi incorporano la protezione nel nucleo del sistema, ma gli aggressori trovano il modo di aggirarla. È la natura del dinamico panorama delle minacce informatiche, che non cambierà mai. Ma i progressi nel settore della sicurezza delle informazioni e dei sistemi operativi spingeranno gli autori di malware a tralasciare i sistemi per attaccare direttamente l'hardware?

Le recenti versioni di Windows hanno incluso la protezione dall'esecuzione di dati, oltre che la casualizzazione dello spazio degli indirizzi (address-space layout randomization). Questi metodi di protezione rendono più difficile per un aggressore compromettere un computer. Negli ultimi anni, anche le tecnologie di crittografia hanno potenziato la protezione dei sistemi operativi. Con la maggior parte delle misure di protezione interne ai sistemi operativi, gli aggressori hanno trovato molto rapidamente modi per eluderle. Con il prossimo rilascio di Windows 8, Microsoft includerà molte nuove funzioni di sicurezza: archiviazione protetta delle password, funzioni di avvio sicuro, difese antimalware e anche migliori funzioni basate sulla reputazione. Con questa nuova architettura di protezione dove si volgeranno gli aggressori?

La risposta è "in profondità e fuori": in profondità nell'hardware e fuori dal sistema operativo.

Negli ultimi anni McAfee Labs ha osservato una grande evoluzione da parte degli aggressori e degli autori di malware, sia per quanto riguarda i rootkit che i bootkit. I rootkit sono usati per sovvertire sia il sistema operativo che il software di sicurezza, mentre i bootkit attaccano la crittografia e possono sostituire il legittimo avvio del sistema. Si tratta di tecniche avanzate per l'intercettazione di password e chiavi di crittografia e per sovvertire anche le difese basate sulla firma dei driver e impiegate da alcuni sistemi operativi.

Attaccare hardware e firmware non è facile, ma avere successo in questo ambito consentirebbe agli aggressori di creare "immagini" del malware persistenti in schede di rete, dischi rigidi e perfino nei BIOS di sistema. Per tutto il 2012 e oltre prevediamo un maggiore impegno negli exploit hardware e firmware e nei correlati attacchi al mondo reale.

I progressi nella funzione di avvio sicuro di Windows 8 hanno già indotto i ricercatori a mostrare come tali progressi possono essere annullati dai BIOS obsoleti; nel frattempo, il prodotto non è neanche stato pienamente rilasciato. Con l'ulteriore sviluppo delle specifiche di interfaccia firmware unificate ed estendibili di Intel - concepite come un'interfaccia software fra il sistema operativo e il firmware della piattaforma per garantire un avvio sicuro e per sostituire i BIOS obsoleti - ci aspettiamo che nei prossimi anni un maggior numero di aggressori investirà il suo tempo nel cercare il modo di eludere queste difese.

Osserveremo con attenzione come gli aggressori utilizzano queste funzioni di basso livello per il controllo delle botnet, forse spostando le loro funzioni di controllo all'interno di funzioni del processore grafico, del BIOS o del master boot record (MBR). Allo stesso tempo prevediamo che gli aggressori sfrutteranno "nuovi" standard di protocollo come IPv6 man mano che le implementazioni di rete evolvono in linea con i sistemi operativi.

Nonostante i nostri sforzi di ridurre le loro ambizioni, gli aggressori hanno ben chiari la convenienza e la potenza di un attacco all'hardware, per cui usciranno dal campo dei tradizionali attacchi al sistema operativo.

Informazioni sugli autori

Questo report è stato preparato e redatto da Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Permeh, Craig Schmugar, Jimmy Shah, Peter Szor, Guilherme Venere e Adam Wosotowsky di McAfee Labs.

Informazioni su McAfee Labs

McAfee Labs è il gruppo di ricerca globale di McAfee. Con l'unica organizzazione di ricerca focalizzata su tutti i vettori di minaccia, ovvero malware, web, e-mail, rete e vulnerabilità, McAfee Labs raccoglie l'intelligence dai propri milioni di sensori e dal suo servizio McAfee Global Threat Intelligence™ basato su cloud. I 350 ricercatori pluridisciplinari di McAfee Labs in 30 nazioni seguono la gamma completa di minacce in tempo reale, identificando le vulnerabilità delle applicazioni, analizzando e correlando i rischi e attivando rimedi immediati per proteggere aziende e consumatori.

Informazioni su McAfee

McAfee, società interamente controllata da Intel Corporation (NASDAQ:INTC), è la principale azienda focalizzata sulle tecnologie di sicurezza. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di collegarsi a Internet, navigare ed effettuare acquisti sul web in modo sicuro. Supportata dal suo ineguagliato servizio di Global Threat Intelligence, McAfee crea prodotti innovativi destinati a utenti consumer, aziende, pubblica amministrazione e service provider che necessitano di conformarsi alle normative, proteggere i dati, prevenire le interruzioni dell'attività, individuare le vulnerabilità e monitorare e migliorare costantemente la propria sicurezza. McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti. http://www.mcafee.com/it

[1] https://blogs.mcafee.com/mcafee-labs/stuxnet-update
[2] La versione non riservata è consultabile all'indirizzo http://www.defense.gov/news/d20110714cyber.pdf

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

40302rpt_threat-predictions_1211_fnl_ETMG