Indice dei contenuti

1. Malware mobile 3
2. Valute virtuali 3
3. Crimine informatico e guerra informatica 4
4. Attacchi social 4
5. Attacchi contro PC e server 4
6. Big data 5
7. Attacchi sul cloud 5
Informazioni sugli autori 6
Informazioni su McAfee Labs 6

1. Il malware mobile sarà il motore di crescitaper innovazione tecnica e volume degli attacchi nel "mercato" complessivo del malware nel 2014.

Nel 2013 il tasso di crescita nella comparsa di nuovo malware mobile, che colpisce quasi esclusivamente la piattaforma Android, è stato di gran lunga superiore a quello del nuovo malware rivolto ai PC. Negli ultimi due trimestri riportati, la crescita del nuovo malware contro i PC è rimasta stabile, mentre la comparsa di nuovi campioni Android è salita del 33%.

Sebbene McAfee Labs preveda che questo trend continuerà anche nel 2014, non sarà solo il tasso di crescita nei nuovi attacchi mobile a fare notizia. Si prevede di assistere a tipologie di attacchi completamente nuovi rivolti contro Android. È estremamente probabile che vedremo i primi veri attacchi ransomware rivolti ai dispositivi mobili che crittografano i dati fondamentali sul dispositivo e li trattengono in cambio di un riscatto. Le informazioni saranno restituite solo se la vittima paga all'esecutore un riscatto in valuta convenzionale o virtuale, come Bitcoin. Altre nuove tattiche che prevediamo faranno la loro comparsa nel mondo mobile includono attacchi sulle vulnerabilità delle funzioni NFC (Near-Field Communications) ora rilevate su molti dispositivi e attacchi che contaminano app valide per appropriarsi dei dati senza essere rilevati.

Gli attacchi contro i dispositivi mobili, prenderanno di mira anche l'infrastruttura delle grandi aziende. Questi attacchi saranno facilitati dall'ormai diffuso fenomeno del BYOD (Bring Your Own Device) unitamente alla relativa immaturità della tecnologia di sicurezza mobile. Gli utenti che scaricano inconsapevolmente malware introdurranno all'interno del perimetro aziendale malwareprogettato per esfiltrare dati riservati. Il fenomeno del BYOD non sta scomparendo, perciò le aziende devono mettere in essere policy e soluzioni complete per la gestione dei dispositivi per evitare di diventare vittime.

2. Le valute virtuali alimenteranno attacchi ransomware sempre più pericolosi in tutto il mondo.

Gli attacchi ransomware che crittografano i dati sui dispositivi delle vittime ci hanno accompagnato per un certo periodo. Tuttavia, tali attacchi sono stati storicamente vulnerabili alle azioni delle forze dell'ordine adottate contro i processori di pagamenti utilizzati dagli esecutori.

Casella di dialogo CryptoLocker.

Sebbene la crescita nell'utilizzo di valute virtuali benefici e promuova attività economica, la stessa ha anche fornito ai criminali informatici la perfetta infrastruttura di pagamento anonima e assolutamente senza regole di cui hanno bisogno per raccogliere il denaro dalle loro vittime. Prevediamo che attacchi come CryptoLocker prolifereranno finché tali attacchi rimarranno (molto) redditizi. Prevediamo inoltre di vedere nuovi attacchi ransomware rivolti contro le aziende che pretenderanno di crittografare le principali risorse dati aziendali.

La buona notizia sia per i singoli che per le aziende è che sebbene il payload del ransomware sia unico, i meccanismi di distribuzione (spam, download drive-by e app infette) non lo sono. Consumatori e aziende che mantengono aggiornati i loro sistemi antimalware (endpoint e reti) saranno relativamente al sicuro da questa minaccia. Un sistema di backup efficace, che sia personale o implementato in azienda, isolerà le vittime dalle conseguenze più negative del ransomware.

3. Nel mondo spia contro spia del crimine informatico e della guerra informatica, le gang criminali e gli attori di stato distribuiranno nuovi attacchi furtivi che saranno più difficili che mai da identificare e bloccare.

Le soluzioni di sicurezza informatica sono diventate sempre più sofisticate e lo stesso hanno fatto gli sforzi della comunità di criminali informatici per eludere tali difese. Gli attacchi che includono le tecniche di evasione avanzate rappresentano il fronte più nuovo nella guerra della sicurezza dei dati enterprise. Una tecnica di evasione popolare che sarà ampiamente adottata dai criminali informatici nel 2014 è l'impiego di attacchi sandbox-aware che non si distribuiscono in modo completo finché non ritengono di essere eseguiti direttamente su un dispositivo non protetto.

Altre tecnologie di attacco popolari che saranno sviluppate e distribuite ulteriormente nel 2014 includono attacchi di programmazione return-oriented che spingono applicazioni legittime a comportarsi in modi dannosi, malware che si cancella da solo che copre le sue tracce dopo aver corrotto un obiettivo e attacchi avanzati sui sistemi di controllo industriale dedicati che hanno il potenziale di danneggiare infrastrutture pubbliche e private.

Gli attacchi con motivazioni politiche continueranno ad aumentare, in particolare nel periodo delle Olimpiadi invernali del 2014 di Sochi (Febbraio) e della coppa del mondo di calcio FIFA World Cup in Brasile (Giugno-Luglio). Anche gli attivisti informatici sfrutteranno tali eventi per promuovere le loro idee.

I dipartimenti IT delle aziende dovranno rispondere a questa nuova serie di tattiche per garantire che le loro difese non dipendano completamente da misure di sicurezza che possano essere facilmente superate da gruppi globali di criminali informatici.

4. Gli attacchi social saranno onnipresenti entro la fine del 2014.

Gli attacchi alle piattaforme social sono quelli che sfruttano le ampie basi di utenti di Facebook, Twitter, LinkedIn, Instagram, ecc. Molti di questi attacchi imiteranno le tattiche del malware legacy come Koobface e semplicemente utilizzeranno le piattaforme social come meccanismo di consegna. Nel 2014, tuttavia, prevediamo di assistere anche ad attacchi che utilizzano funzionalità uniche delle piattaforme social per distribuire dati relativi a contatti, ubicazioni o attività commerciali che possono essere utilizzati per mirare meglio la pubblicità o perpetrare crimini virtuali o nel mondo reale.

Uno dei più comuni attacchi contro tali piattaforme semplicemente ruba le credenziali di autenticazione degli utenti, che vengono poi utilizzate per estrarre dati personali da "amici" e colleghi ignari. La botnet Pony[1], che ha rubato più di due milioni di password dagli utenti di Facebook, Google, Yahoo e altri, è solo la punta dell'iceberg. Facebook stessa stima che 50-100 milioni dei suoi account MAU (utenti attivi mensili) siano duplicati e che fino a 14 milioni dei MAU registrati siano considerati "sgraditi". In base a un recente studio Stratecast, il 22% degli utenti di social media sono stati vittime di un incidente legato alla sicurezza[2].

Aziende pubbliche e private sfrutteranno le piattaforme social per eseguire "attacchi di ricognizione" contro i propri concorrenti e rivali, direttamente o tramite terze parti. Nel corso del 2013 leader di alto profilo nei settori pubblico e privato sono stati presi di mira da tali attacchi. Possiamo prevedere che la frequenza e l'ampiezza di questi attacchi si estenderà nel corso del 2014.

L'altra forma di attacchi social cui prevediamo di assistere in volume nel 2014 saranno gli attacchi "sotto falsa bandiera" che ingannano gli utenti spingendoli a rivelare informazioni personali o credenziali di autenticazione. Uno degli attacchi più popolari presenterà una richiesta "urgente" di reimpostare la password dell'utente. Al contrario ruberà nome utente e password e quindi utilizzerà l'account dell'utente ignaro per raccogliere informazioni personali sull'utente stesso e sui suoi contatti.

Prevenire gli attacchi contro le piattaforme social e quelli sotto falsa bandiera richiederà una maggiore vigilanza da parte dei singoli e delle policy e soluzioni aziendali per garantire che l'uso delle piattaforme di social media da parte dei dipendenti non comporti violazioni di dati materiali.

5. Nuovi attacchi contro PC e server si rivolgeranno contro vulnerabilità sopra e sotto il sistema operativo.

Mentre molte unioni di criminali informatici riporranno la loro attenzione verso i dispositivi mobili, altri continueranno a prendere di mira PC e piattaforme server. Tuttavia, i nuovi attacchi cui assisteremo nel 2014 non si limiteranno ad attaccare il sistema operativo, ma sfrutteranno anche le vulnerabilità presenti al di sopra e al di sotto dello stesso.

Molti dei nuovi attacchi contro PC nel 2014 sfrutteranno le vulnerabilità in HTML5, che permette ai siti web di ravvivarsi con interazione, personalizzazione e ricche possibilità per i programmatori. Tuttavia, HTML5 presenta una serie di nuove superfici d'attacco. Utilizzando HTML5 i ricercatori hanno già mostrato come monitorare la cronologia del browser dell'utente per meglio mirare la pubblicità. Poiché molte applicazioni basate su HTML5 sono progettate per i dispositivi mobili, prevediamo di assistere ad attacchi che violeranno la sandbox del browser e daranno agli aggressori accesso diretto al dispositivo e ai suoi servizi. Molte aziende realizzeranno inoltre applicazioni aziendali basate su HTML5. Per prevenire l'esfiltrazione dei dati utilizzati da queste app, la sicurezza dovrà essere incorporata in questi nuovi sistemi fin da subito.

I criminali informatici prenderanno sempre più di mira le vulnerabilità presenti al di sotto del sistema operativo nello stack storage e anche nel BIOS. Per mitigare questi attacchi nell'ambiente aziendale sarà necessario sviluppare misure di sicurezza basate su hardware che operano anche al di sotto del livello del sistema operativo.

6. Il mutevole panorama delle minacce costringerà all'adozione di analitiche di sicurezza dei big data per soddisfare i requisiti relativi a rilevamento e prestazioni.

Storicamente la maggior parte delle soluzioni di sicurezza delle informazioni si sono basate sull'identificazione di payload pericolosi (blacklisting) o sulla localizzazione di applicazioni notoriamente valide (blacklisting). La sfida attuale che i professionisti della sicurezza si trovano ad affrontare prevede l'identificazione e la corretta elaborazione di payload "grigi". Ciò comporta l'applicazione di molteplici tecnologie di sicurezza unitamente a servizi di reputazione delle minacce efficaci.

I servizi di reputazione delle minacce hanno già dimostrato il loro valore nel rilevamento di malware, siti web pericolosi, spam e attacchi di rete. Nel 2014 i fornitori di sicurezza aggiungeranno nuovi servizi di reputazione delle minacce e strumenti analitici che permetteranno loro e ai loro utenti di identificare le minacce persistenti avanzate e furtive in modo più rapido e preciso di quanto sia oggi possibile. Le analitiche dei big data permetteranno ai professionisti della sicurezza di identificare i sofisticati attacchi con tecniche avanzate di evasione e le minacce persistenti avanzate che possono compromettere i processi aziendali più strategici.

7. La distribuzione di applicazioni aziendali basate sul cloud creerà nuove superfici d'attacco che saranno sfruttate dai criminali informatici.

Willie Sutton, che si dice abbia rapinato 100 banche all'inizio del 20° secolo, è famoso per aver sottolineato che derubava le banche perché "è lì che si trova il denaro"[3]. Le bande di criminali informatici del 21° secolo prenderanno di mira le applicazioni basate su cloud e i repository di dati perché è lì che si trovano i dati, o avverrà presto. Questo potrebbe avvenire tramite applicazioni aziendali che non sono state valutate dall'IT in base alle policy di sicurezza aziendali. In base a un recente report, oltre l'80% degli utenti aziendali utilizza applicazioni cloud senza che il dipartimento IT dell'azienda ne sia al corrente o senza il loro supporto[4].

Sebbene le applicazioni basate su cloud presentino sicuramente vantaggi funzionali ed economici convincenti, presentano anche una nuova famiglia di superfici di attacco agli aggressori come hypervisor onnipresenti che si trovano in tutti i centri dati, l'infrastruttura di comunicazione multi-tenant implicita nei servizi cloud e l'infrastruttura di gestione utilizzata per fornire e monitorare servizi cloud su larga scala. Il problema per i professionisti della sicurezza aziendale è che quando un'applicazione aziendale passa nel cloud, l'azienda perde visibilità e controllo del profilo di sicurezza.

Questa perdita di controllo diretto del perimetro di sicurezza aziendale pone una forte pressione sui responsabili e sugli amministratori della sicurezza affinché si assicurino che l'accordo di utilizzo e le procedure operative del fornitore cloud garantiscano misure di sicurezza attive e costantemente aggiornate per essere in grado di affrontare il mutevole panorama delle minacce. Le grandi aziende possono avere una leva sufficiente per richiedere ai fornitori di cloud d implementare misure di sicurezza che siano coerenti con la postura di sicurezza dell'azienda stessa. I consumatori più piccoli di servizi cloud, tuttavia, non ne avranno la forza e dovranno esaminare con attenzione gli accordi di utilizzo spesso ambigui dei fornitori in particolare relativamente alla proprietà dei dati e alla sicurezza. I nuovi servizi cloud possono inoltre presentare nuove superfici d'attacco finché i servizi non raggiungono un livello di maturità che include la strumentazione e le contromisure richieste per garantire la sicurezza dei dati che devono proteggere.

Informazioni sugli autori

Questo report è stato preparato e redatto da Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky e Chong Xu.

Informazioni su McAfee Labs

McAfee Labs è la principale fonte mondiale per la ricerca sulle minacce, informazioni sulle minacce e sulla sicurezza informatica. Il team di 500 ricercatori di McAfee Labs raccoglie dati sulle minacce da milioni di sensori tra i principali vettori di minacce: file, web, messaggi e rete. Quindi esegue analisi di correlazione delle minacce su più vettori e offre informazioni sulle minacce in tempo reale per integrarsi con i prodotti di sicurezza McAfee per endpoint e reti tramite il suo servizio cloud McAfee Global Threat Intelligence. McAfee Labs sviluppa anche tecnologie fondamentali per il rilevamento delle minacce - come DeepSAFE, profilazione delle applicazioni e gestione delle graylist - che sono incorporate all'interno del più ampio portafoglio di prodotti di sicurezza del settore.

A proposito di McAfee

McAfee, società interamente controllata da Intel Corporation (NASDAQ: INTC), permette a imprese, enti pubblici e utenti privati di godere dei vantaggi di Internet in tutta sicurezza. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi, reti e dispositivi mobili in tutto il mondo. Grazie alla strategia visionaria Security Connected, a un approccio innovativo nella creazione di soluzioni sempre più sicure e all'ineguagliata rete Global Threat Intelligence, McAfee è impegnata senza sosta a ricercare nuovi modi per mantenere protetti i propri clienti. www.mcafee.com/it

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, "*The Hidden Truth Behind Shadow IT*" *(La verità nascosta dietro la Shadow IT)*. Novembre 2013. http://www.mcafee.com/it/resources/reports/rp-six-trends-security.pdf

[3] Lo stesso Sutton afferma di non aver mai fatto l'affermazione che gli viene attribuita, spiegando invece che rapinava le banche perché "si divertiva".

[4] Stratecast, "*The Hidden Truth Behind Shadow IT*" *(La verità nascosta dietro la Shadow IT)*. Novembre 2013. http://www.mcafee.com/it/resources/reports/rp-six-trends-security.pdf

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

60756rpt_threats-predictions_1213_fnl_ETMG