Rapporto

Previsioni sulle minacce per il 2011

Di McAfee® Labs™

Il panorama delle minacce si è evoluto in modo considerevole nello scorso anno. McAfee Labs ha osservato aumenti netti nella complessità e nella precisione nell'individuare gli obiettivi del malware oltre ad un costante aumento nel volume complessivo quotidiano delle minacce malware. Abbiamo inoltre iniziato ad assistere a modifiche significative nelle tipologie di minacce rivolte a colpire i dispositivi Apple iPhone e altri dispositivi mobile. Ma ci sono anche delle buone notizie, in primo luogo un calo significativo della quantità quotidiana di spam che combattiamo. Queste oscillazioni ci portano a chiederci come stanno evolvendo queste minacce.

Come abbiamo fatto negli ultimi anni, McAfee Labs è pronta a rispolverare la sfera di cristallo per offrire intrepide previsioni sulle minacce per il prossimo anno e quelli a venire. Ti consigliamo di prendere in considerazione questi suggerimenti per prepararti per le minacce del futuro in costante evoluzione.

Indice dei contenuti

Lo sfruttamento dei social media

Nel 2010 abbiamo rilevato alcuni cambiamenti significativi nel modo in cui codice e link malevoli vengono distribuiti. Quest'anno si è concluso con alcuni dei livelli complessivi di spam più bassi da anni, poiché sempre più utenti passano da strumenti di comunicazione legacy "più lenti" come la posta elettronica a metodi più immediati come l'instant messaging e Twitter. Questo passaggio modificherà completamente il panorama delle minacce nel 2011.

"Le connessioni dei social media probabilmente sostituiranno la posta elettronica come vettore principale per la distribuzione di codice e link malevoli".

Dal momento che sia gli utenti consumer che quelli aziendali continuano ad affollare social media e siti di socializzazione per comunicazioni istantanee e condividere i dati, ci aspettiamo di assistere ad abusi sempre più mirati dell'identità e dei dati personali. Le connessioni dei social media probabilmente sostituiranno la posta elettronica come vettore principale per la distribuzione di codice e link malevoli. L'enorme quantità di informazioni personali online unitamente al fatto che l'utente non sa come proteggere tali dati renderà estremamente più semplice che mai per i criminali informatici perpetrare furti d'identità e attività di profilazione dell'utente. Lo spear phishing - attacchi di phishing mirati - si sposterà su Twitter e tecnologie similari dal momento che diventa semplice scegliere utenti e gruppi da sfruttare attraverso questi canali.

Due aree correlate dei social media catalizzeranno l'attenzione il prossimo anno: gli URL abbreviati e le tecnologie di geolocalizzazione.

Abuso del servizio di Short URL: Gli URL abbreviati hanno un senso quando vengono utilizzati nei social media ed in altre forme. I link abbreviati sono più semplici da incollare o digitare. Il problema - e l'abuso - ne consegue dal momento che gli utenti non sanno dove tali link abbreviati portano realmente finché non ci cliccano sopra. Si tratta di un'enorme opportunità per i malintenzionati. Gli spammer hanno già adottato gli URL abbreviati per aggirare i filtri tradizionali. McAfee Labs prevede che l'abuso degli URL abbreviati si estenderà anche in altre forme di comunicazioni tramite Internet. Attualmente tracciamo ed analizziamo - attraverso varie applicazioni di social media e tutti i servizi di abbreviazione degli URL - oltre 3.000 URL abbreviati al minuto. Ne osserviamo un crescente numero utilizzati per spam, truffe e altri scopi malevoli. Questa comoda tecnica avrà un impatto tremendo sul successo dei criminali informatici e dei truffatori poiché sfruttano l'immediatezza dei social media rispetto all'e-mail per un maggior successo.

Abuso dei servizi di geolocalizzazione: Sempre più utenti Internet di ogni livello aggiungono informazioni di tipo GPS (Sistema di posizionamento globale) ai loro aggiornamenti sui siti social media in modo che i loro amici e colleghi possano sapere dove si trovano. Inoltre, molti servizi di geoposizionamento offrono stemmi e premi per migliorare la loro popolarità. Non è difficile immaginare come i criminali informatici e i truffatori possano potenzialmente sfruttare queste informazioni: servizi come foursquare, Gowalla e Facebook Places permettono di cercare, tracciare e rilevare con facilità dove si trovano amici e sconosciuti. Utilizzando la funzionalità di mappatura di Bing, per esempio, si possono rilevare tutti i tweet abilitati al servizio GPS in un'area specifica. Inoltre, è semplice correlarli per argomento o area di interesse. Con soli pochi click i criminali informatici possono visualizzare in tempo reale chi sta usando Twitter e dove, cosa dicono, i loro interessi e i sistemi operativi e applicazioni che utilizzano. Diventa poi un gioco da ragazzi creare un attacco mirato sulla base di quanto i malintenzionati hanno appreso da questi servizi.

Il fatto che questi servizi consentano a chiunque di vedere e tracciare singoli e gruppi - incluse le loro simpatie ed antipatie, affiliazioni e interessi - e poi agire su di essi in modo rapido, farà si che questo argomento diventerà un bersaglio per criminali informatici e truffatori nel 2011 e oltre.

Mobile

Le minacce contro i dispositivi mobile sono state un argomento caldo all'interno della comunità di sicurezza per molti anni; prevediamo che gli attacchi esploderanno in qualsiasi momento, anche se non sembrano ancora verificarsi. Ciò nonostante, McAfee Labs prevede che il 2011 sarà un punto di svolta per le minacce volte a colpire i dispositivi mobile. Quest'anno abbiamo visto molte nuove minacce, ma poco diffuse, contro i dispositivi mobile: rootkit per la piattaforma Android, exploit "jailbreaking" remoti per l'iPhone e l'arrivo di Zeus (Trojan/botnet di tipo bancario molto noto). La diffusa adozione dei dispositivi mobile in ambienti aziendali combinati con questi ed altri attacchi probabilmente porterà a quest'esplosione che abbiamo da tempo previsto. Data la nostra infrastruttura cellulare storicamente debole e i lenti progressi in termini di crittografia, i dati degli utenti e aziendali possono trovarsi ad affrontare rischi seri.

Apple

Qualsiasi professionista della sicurezza che consulta online i forum di InfoSec o partecipa alle loro conferenze saprà che la piattaforma Mac OS X è uno degli obiettivi preferiti delle comunità di hacker malintenzionati e di hacker etici. Gli hacker etici hanno giocherellato con il Mac per molto tempo alla ricerca di vulnerabilità. Sebbene storicamente non sia una piattaforma frequentemente presa di mira dagli aggressori malevoli, il sistema operativo Mac è davvero ampiamente diffuso. Quest'anno, McAfee Labs ha osservato malware sempre più sofisticato mirato a colpire le piattaforme Mac; prevediamo che questo trend aumenterà nel 2011. La popolarità di iPad e iPhone negli ambienti aziendali e la facile portabilità del codice malevolo tra di loro potrebbe mettere in pericolo molti utenti e aziende nei prossimi anni. Prevediamo che le minacce contro dati e identità saranno in aumento. La mancanza di comprensione da parte degli utenti relativamente alla vulnerabilità di queste piattaforme e il non aver implementato soluzioni di sicurezza li rende un terreno fertile per i criminali informatici. McAfee Labs prevede che nel 2011 botnet e Trojan diventeranno sempre più comuni sulle piattaforme Apple.

Applicazioni

Indipendentemente dalla piattaforma o dispositivo scelto, viviamo in un modo incentrato sulle applicazioni. L'inconveniente di tale mondo risiede nella portabilità delle nostre applicazioni tra i dispositivi mobile e le prossime piattaforme di Internet TV, la cui combinazione renderà le minacce in arrivo da applicazioni vulnerabili e malevoli una delle principali preoccupazioni per il 2011. Oltre al codice malevolo, McAfee Labs prevede applicazioni che mirano a colpire o rivelano dati d'identità e privacy. Questo pericolo potrebbe portare ad una vulnerabilità dei dati e a minacce attraverso nuove piattaforme media come Google TV.

"La premura di vendere prodotti insicuri porterà nel 2011 ad attacchi contro la privacy e i dati più centrati sulle applicazioni".

Dal momento che le applicazioni per il controllo dei dispositivi, a casa e in ufficio, diventano più popolari si trasformeranno sempre più in obiettivi. Questi strumenti storicamente dispongono di una codifica e pratiche di sicurezza deboli, e consentiranno ai criminali informatici di manipolare una gamma di dispositivi fisici attraverso applicazioni compromesse o controllate. Questa aggressione porterà l'efficacia delle botnet a un nuovo livello.

Nel 2011, McAfee Labs prevede un numero crescente di applicazioni sospette e malevoli per le piattaforme e i sistemi operativi mobile più diffusamente implementati. Le applicazioni mal sviluppate hanno già rivelato dati relativi all'identità. Prevediamo che sviluppatori e addetti marketing soccomberanno al modo di pensare "rush to market" nel momento in cui tali applicazioni diventano più comuni. Sono particolarmente a rischio quelle piattaforme che hanno modelli di sviluppo e distribuzione delle applicazioni poco supervisionati. Questa premura di vendere prodotti insicuri potrebbe portare nel 2011 ad attacchi contro la privacy e i dati più centrati sulle applicazioni.

Quest'anno McAfee Labs ha già osservato uno spostamento verso botnet controllate dalle applicazioni in Twitter e LinkedIn; prevediamo che questa sarà la norma nel 2011 e oltre, dal momento che l'implementazione e l'utilizzo delle applicazioni diventano sempre più diffuse. Sarà questo l'anno delle botnet mobile controllate attraverso un'applicazione scaricata online?

La sofisticazione si confonde con la legittimità

Quest'anno abbiamo registrato una maggior complessità di alcune minacce. Il malware cosiddetto "signed" (ovvero firmato) che imita file legittimi sarà sempre più diffuso nel 2011. Ciò causerà un aumento del furto di chiavi e delle tecniche e strumenti per creare chiavi fasulle da utilizzare in questi tipi di attacchi.

Gli attacchi di "fuoco amico" - in cui le minacce sembrano arrivare dai propri amici - da social media come Koobface e VBMania continueranno ad aumentare. Ciò andrà di pari passo con l'aumentato abuso dei social network, che probabilmente sostituiranno la posta elettronica quale vettore principale per le minacce.

Prevediamo inoltre di assistere a un aumento degli attacchi "smart bomb", ovvero designati a scatenarsi in base a determinate condizioni e non altre. Queste minacce richiedono che le vittime seguano il percorso d'attacco designato - contrastando honeypot, crawler e ricercatori di sicurezza - incidendo in modo significativo sugli obiettivi designati e vulnerabili. Tali minacce creeranno un'esigenza ancor più grande di informazioni Global Threat Intelligence per proteggersi contro gli attacchi osservati in circostanze specifiche.

Gli attacchi personalizzati sono in procinto di diventare sempre più personali.

La sopravvivenza delle botnet

Come menzionato nella parte relativa alle applicazioni, le botnet continueranno ad essere una delle maggiori e più sofisticate minacce che McAfee Labs si trova ad affrontare. Nei prossimi anni, prevediamo di vedere maggiori funzionalità di esfiltrazione dei dati. Nel corso di quest'anno abbiamo osservato i criminali informatici coinvolti in un crescente numero di attacchi mirati; prevediamo una maggior focalizzazione sulle botnet che rimuovono i dati da macchine e aziende mirate, piuttosto che sulla pratica comune dell'invio di spam. Le botnet saranno anche coinvolte in funzionalità avanzate di raccolta dei dati e saranno più focalizzate sul colpire ed abusare i siti di social networking.

Anche le botnet subiscono delle perdite. Le forze dell'ordine in tutto il mondo hanno di recente chiuso Mariposa, Bredolab e alcune botnet Zeus. Tuttavia, le botnet continuano ad evolvere. Prevediamo che la recente fusione di Zeus con SpyEye produrrà bot più sofisticate dati i miglioramenti conseguiti nell'aggirare i meccanismi di sicurezza e il monitoraggio delle forze dell'ordine. E così anche fusioni ed acquisizioni hanno fatto il loro ingresso nel mondo del malware.

Le botnet che utilizzano Facebook e Twitter amplieranno la loro portata ed includeranno siti popolari di social networking come foursquare, Xing, Bebo, Friendster e altri. Il crescente numero di utenti e l'utilizzo in azienda di questi siti è qualcosa che i criminali informatici non possono ignorare. McAfee Labs prevede inoltre una maggiore integrazione di funzioni basate sulla geolocalizzazione all'interno delle botnet poiché le funzioni GPS diventano sempre più diffuse.

Hacktivism

Gli attacchi motivati da ragioni politiche non sono una novità, ma li incontriamo sempre più regolarmente. E saranno sempre più numerosi nel 2011. Oltre alla tecnica del defacciamento (la principale attività degli hacker attivisti) e attacchi DDoS (Distributed Denial of Service, la più recente attività "di moda"), faranno la loro apparizione nuovi tipi di attacchi sofisticati. Il furto di informazioni, rubate e poi divulgate per screditare avversari politici, aumenterà sicuramente. Un numero maggiore di gruppi seguirà l'esempio di Wikileaks, poiché la pratica dell'hacktivism è condotta da persone che dichiarano di essere indipendenti da qualsiasi governo o movimento. Che i governi guidino segretamente tali manipolazioni e attività è un dibattito aperto, ma è abbastanza probabile che gli stati adotteranno un modello piratesco. L'hacktivism come diversivo potrebbe essere il primo passo verso la guerra cibernetica. Chiunque all'interno del mondo della sicurezza informatica - dai giornalisti ai ricercatori - dovranno essere attenti nel riconoscere la differenza tra hacktivism e l'inizio di una guerra cibernetica.

"L'hacktivism diventerà il nuovo modo per dimostrare la propria posizione politica nel 2011".

Prevediamo che i social network saranno utilizzati più spesso per far entrare in gioco l'hacktivism il prossimo anno. Proprio come il crimine informatico è passato da individui isolati (in grado di creare malware) a gruppi non strutturati (in grado di lanciare un attacco DDoS), prevediamo che nel 2011 ci sarà un numero sempre maggiore e più solido di organizzazioni e strutture all'interno dei gruppi di hacker attivisti.

L'hacktivism diventerà il nuovo modo per dimostrare la propria posizione politica nel 2011 e oltre. Abbandonando le strade, gli organizzatori politici passeranno a Internet per lanciare attacchi e inviare messaggi alla luce del giorno o nel tempo di Internet. E, come nel mondo fisico, prevediamo che gli attacchi da parte di hacktivist ispireranno e fomenteranno rivolte e altre dimostrazioni del mondo reale.

Minacce avanzate persistenti

La notizia di gennaio dell'incidente Operazione Aurora/Google ha dato vita ad una nuova categoria di minacce avanzate persistenti (Advanced Persistent Threat o APT), un argomento di dibattito nel settore e sulla stampa per buona parte dell'anno. Tuttavia, esiste molta confusione relativamente alla reale natura di questi attacchi.

La definizione comune di un APT è quella che descrive un attacco di spionaggio o sabotaggio informatico mirato portato avanti con il sostegno o la guida di uno stato-nazione per un fine diverso da motivazioni puramente finanziarie/criminali o protesta politica. Non tutti gli attacchi APT sono estremamente avanzati e sofisticati, così come non tutti gli attacchi mirati molto complessi e ben eseguiti sono APT. La motivazione del nemico, non il livello di sofisticazione o impatto, sono il principale elemento che differenzia un attacco APT da uno da parte di un criminale informatico o un hacktivist.

Per esempio, l'attacco contro RBS WorldPay che ha portato al furto di 9 milioni di dollari da parte di una banda di criminali informatici dell'Europa dell'Est non era un APT, nonostante il suo livello elevato di sofisticazione e coordinamento. Gli attacchi APT inoltre non vengono lanciati da un unico nemico. Esistono numerosi gruppi di attacco APT dislocati nel mondo, tutti con diversi gradi di capacità e competenze. Così come esistono gruppi di livello A e B nella gerarchia dei criminali informatici organizzati, lo stesso vale per gli APT. Alcuni hanno accesso a un'enorme quantità di risorse (hardware, software e umane) e anche abilità tradizionali di intelligence, sorveglianza e ricognizione. Altri prendono in prestito, rubano o acquistano strumenti preconfezionati offerti e spesso utilizzati da bande radicate di criminali informatici e si comportano in modo simile a queste bande, tranne per il tipo di dati che cercano di sottrarre ai loro obiettivi. Aziende di tutte le dimensioni che hanno un coinvolgimento nella sicurezza nazionale o attività economiche globali importanti (anche marginalmente, come uno studio di avvocati che consiglia a un'azienda di avviare attività in un'altra nazione) dovrebbero prevedere di finire sotto attacchi APT costanti e pervasivi che vanno alla ricerca di archivi di posta elettronica, archivi di documenti, repository di proprietà intellettuale e altri database.

Informazioni sugli autori

Questo rapporto è stato redatto da Dmitri Alperovitch, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget e Craig Schmugar di McAfee Labs.

Informazioni su McAfee Labs™

McAfee Labs è il gruppo di ricerca mondiale di McAfee, Inc. 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, Inc.

Con sede principale a Santa Clara, California, McAfee Inc. è la principale azienda focalizzata sulle tecnologie di sicurezza. McAfee è costantemente impegnata ad affrontare le più difficili sfide legate alla 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 da un pluripremiato team di ricerca, 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. www.mcafee.com/it

McAfee Srl
Via Fantoli 7
20138 Milano Italia
(+39) 02.554171
www.mcafee.com/it

17800rpt_threat-predictions_1110_fnl_ETMG