Smart Security

Combattere le Nuova Generazione di Advanced Malware

White Paper

WatchGuard® Technologies, Inc.
Data di pubblicazione: Aprile 2014

Patch, Signature e Routine di Sicurezza

Nel 2003, il worm "SQL Slammer" ha portato al fermo del traffico Internet in molte parti del mondo per diverse ore [1]. Questo noto worm si rivolge ad una vulnerabilità nota nel database Microsoft SQL per la quale era disponibile una patch sei mesi prima. Le chiavi del suo successo e della sua rapida proliferazione sono state la piccola dimensione, il modo in cui si è rapidamente replicato e la ricerca casuale di nuovi obiettivi da infettare.

Nel corso degli anni successivi i produttori IT hanno risposto a minacce di questo tipo. Ogni mese Microsoft rilascia una serie di aggiornamenti per risolvere le vulnerabilità. Adobe adotta lo stesso modello e le sue hotfix di sicurezza vengono rilasciate ogni giovedì. Anche Cisco fornisce una serie rilevante di correzioni relative alla sicurezza una volta per trimestre. Gli amministratori IT sono invitati ad aggiornare i loro sistemi frequentemente per rimanere aggiornati.

Altre difese comprendono Intrusion Prevention Systems (IPS) che utilizzano deep packet inspection per cercare modelli noti di exploit e sistemi antivirus e di quarantena malware. Regolamenti internazionali come PCI DSS obbligano le aziende a mantenere il loro software antivirus aggiornato con le signature più recenti. Soluzioni per la gestione centralizzata sono utilizzate per garantire che tutti gli utenti abbiano in esecuzione le ultime versioni AV sul loro desktop, laptop, e ora anche i dispositivi mobili con sistema operativo Android. Ma non è abbastanza, ed in questo articolo vi spiegheremo il perché.

Zero Day è il nuovo Campo di Battaglia

Nel campo biomedico, ricercatori e medici hanno capito da tempo che i microbi e i batteri si evolvono nel tempo e diventano più resistenti agli antibiotici. Hanno bisogno di sviluppare nuove e più forti molecole per rimanere efficaci. Allo stesso modo nel mondo della sicurezza informatica, nuove tipologie di malware sono emerse più avanzate e resistenti alle difese tradizionali. Gli aggressori si sono evoluti nel tempo e diventati più intelligenti.

Figura 1: Caratteristica di un Advanced Persistent Threat

Il malware moderno utilizza tecniche **avanzate** come i canali criptati di comunicazione, rootkit a livello kernel e sofisticate capacità di evasione per superare le difese di una rete. Ancora più importante, spesso le minacce sfruttano vulnerabilità zero day: difetti per i quali nessuna patch è ancora disponibile e nessuna signature è stata scritta. Nel 2012, il team WatchGuard LiveSecurity ha messo in guardia da quattro zero day con nuove minacce che potevano venire sfruttate [2]. Nel 2013, abbiamo divulgato avvisi di altri tredici zero day che sono stati attivamente utilizzati.

Questi malware sono spesso **persistenti** e progettati per rimanere attivi. Sono furtivi e nascondono accuratamente le comunicazioni e "vivono" dentro la rete di una vittima il più a lungo possibile, spesso ripulendo le tracce della propria presenza (eliminazione dei registri, utilizzo di crittografia, e collegamenti esclusivi col controllore remoto tramite piccole comunicazioni offuscate).

In molti attacchi vengono fuse combinazioni di tecniche diverse. Gruppi di attaccanti altamente qualificati, motivati e finanziariamente sostenuti rappresentano **minacce** significative perché hanno obiettivi molto specifici in mente, come il guadagno finanziario derivante dal furto di carte di credito e altre informazioni preziose.

Questi nuovi ceppi di malware avanzato sono spesso indicati come **Advanced Persistent Threats (APTs)**.

L'evoluzione da Stuxnet a Duqu evidenzia come le tecniche avanzate utilizzate dagli stati nazionali sono ora utilizzati dagli hacker per trarne guadagno finanziario colpendo tutti, dalle aziende Fortune 500 alle piccole e medie imprese, comprese infrastrutture di enti statali ed il settore industriale.

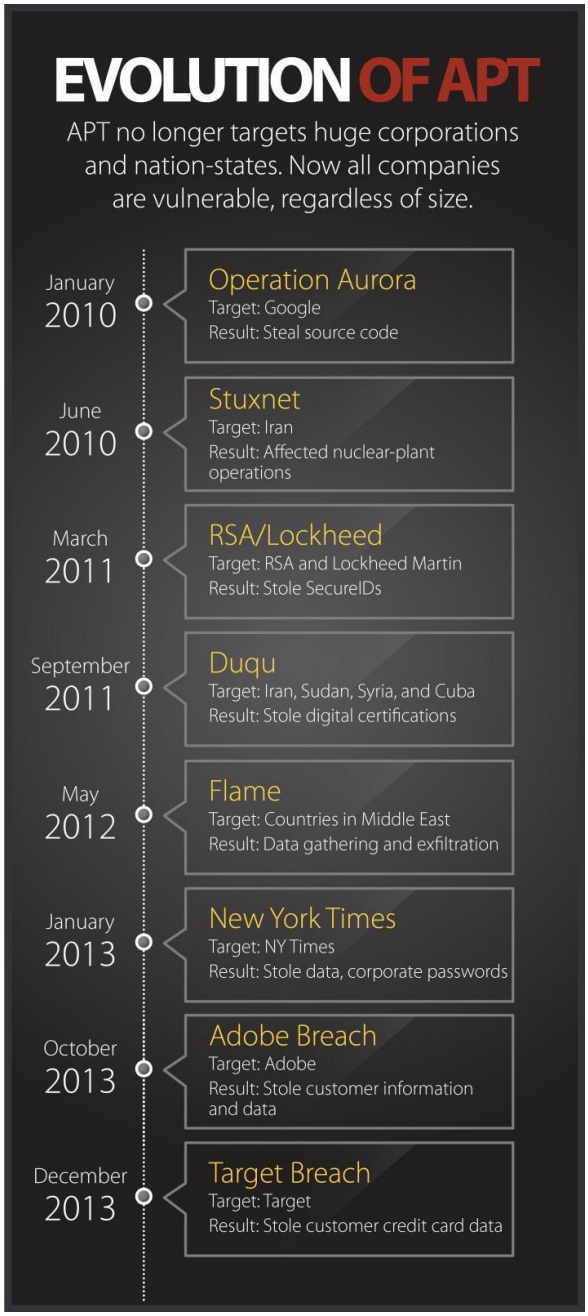

Figura 2: Evoluzione degli APT dal 2010 al 2013

Le conseguenze delle violazioni di sicurezza sono significative per qualsiasi azienda. Forbes ha riferito che le vendite di un grande rivenditore on-line statunitense Target sono diminuite di quasi del 50% nel Q4 del 2013,[3] e la pubblicità intorno ad una violazione di sicurezza subita ai loro dati ne è stato il motivo principale. Il valore delle azioni è sceso del 9%. Il CIO non è più l'azienda, e il 5% -10% degli acquirenti di Target hanno riferito che non faranno più acquisti presso il loro negozio on-line [4].

Anche le difese si stanno evolvendo: Sandbox

La lotta contro il codice malevolo è una corsa agli armamenti. Ogni volta che i difensori introducono nuove tecniche di rilevamento, gli aggressori cercano di trovare nuovi modi per aggirarle. Aziende antivirus tradizionali impiegano ingegneri e signature writers che analizzano i file e verificano l'esecuzione di programmi sconosciuti in un ambiente controllato e monitorato. Oppure possono inviare i file a strumenti come Anubis, che eseguono un file per segnalare eventuali attività sospette o un comportamento che indica un virus.

La scrittura di signature è una proposta inadeguata. L'88% del nuovo malware è una variante di malware esistenti.

Ma la scrittura di signature è una proposta inadeguata perché vi è una probabilità dell' 88% che il nuovo malware è stato creato come una variante di malware esistenti per evitare il rilevamento con tecniche classiche.

Oggi, le soluzioni sandbox vengono utilizzati automaticamente come parte del processo di rilevamento. Il codice viene eseguito e analizzato in modo dinamico nella sandbox, senza alcuna supervisione umana. Tuttavia gli autori di malware utilizzano anche tecniche evasive per garantire che i loro programmi non vengano individuati come attività dannose quando eseguiti in un ambiente di analisi automatizzata. Alcune tecniche più comuni utilizzate dal malware sono:

- **Controlla la presenza** di una macchina virtuale
- **Controlla chiavi di registro note di Windows** che indicano una particolare sandbox
- **Rimani silente** in attesa del timeout di analisi della sandbox

I fornitori di sicurezza hanno reagito con l'aggiunta di tecniche di contro-spionaggio per i loro sistemi. Controllano le richieste alle chiavi di registro e costringono un programma a riattivarsi dopo aver inviato una richiesta TSR (Terminate and Stay Resident). Ma questo approccio è ancora di tipo reattivo. Sistemi di analisi del malware devono essere aggiornati manualmente per gestire ogni nuova evasione. Gli autori di malware che creano evasioni zero day possono ignorare il rilevamento fino a quando la sandbox non viene aggiornata

"Oltre la SandBox" - Emulazione Completa di Sistema

Le implementazioni sandbox più comuni oggi in genere si basano su un ambiente virtuale che contiene un sistema operativo ospite. In questi casi la sandbox esegue il sistema

operativo direttamente su una macchina reale. Il problema chiave, che rappresenta anche la limitazione fondamentale delle sandbox moderne basate sulla virtualizzazione, è la loro mancanza di visibilità e comprensione l'esecuzione di un programma malware. La sandbox deve vedere gran parte del comportamento delle minacce informatiche ma deve farlo in un modo che si nasconda dal malware stesso. Se il malware è in grado di rilevare la presenza di una sandbox, modifica il suo comportamento.

Ad esempio, invece di terminare e rimanere residenti, programmi sofisticati eseguono calcoli (al solo scopo evasivo) al fine di dare un'apparenza di attività. Quindi, non vi è alcun modo per la sandbox di riattivare il programma. Dal punto di vista del sistema di analisi del malware, tutto è normale.

La maggior parte del malware viene eseguito in modalità utente (sia come utente normale o amministratore). Sandbox basate sulla virtualizzazione eseguono le chiamate API di Windows e chiamate di sistema in modalità utente. Le chiamate di sistema o di funzione catturano le interazioni tra un programma e il suo ambiente (ad esempio quando i file vengono letti, chiavi di registro scritte e viene generato traffico di rete). Ma la sandbox non può individuare tutto ciò che accade tra le chiamate di sistema e gli autori di codice malware possono indirizzarsi in questa zona cieca. È quindi necessario un approccio più intelligente. Un emulatore è un programma software che simula la funzionalità di un altro programma o un pezzo di hardware. Dal momento che un emulatore implementa le funzionalità a livello software, fornisce una grande flessibilità.

L'emulazione del sistema operativo nel sistema operativo fornisce un elevato livello di visibilità dei comportamenti dei malware. Ma emulatori a livello di sistema operativo non possono replicare ogni chiamata ad un sistema operativo. Essi in genere si concentrano su un sottoinsieme noto di funzionalità. Sfortunatamente, questo approccio è il più facile per il malware avanzato da rilevare ed eludere.

La piena emulazione sistema, dove l'emulatore simula l'hardware fisico (inclusi CPU e memoria), fornisce il livello più profondo di visibilità sul comportamento del malware, ed è anche il più difficile per il malware avanzato da rilevare.

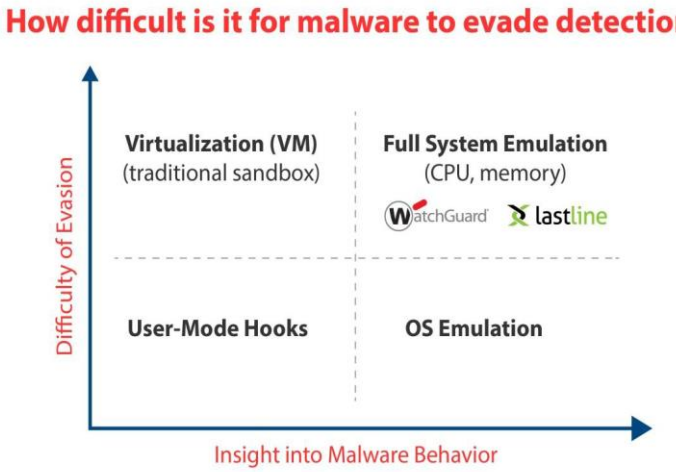

Figura 3: L'emulazione completa di sistema ha la migliore individuazione di malware

WatchGuard Blocker APT

APT Blocker, un nuovo servizio disponibile per tutte le appliance WatchGuard UTM, utilizza l'emulazione completa del sistema (CPU e memoria) per verificare dettagliatamente l'esecuzione di un programma malware. Dopo la prima esecuzione attraverso altri servizi di sicurezza, viene creata l'impronta del file (Hash) e confrontata con un database esistente prima nel dispositivo UTM e poi nel cloud. Se il file non è mai stato visto prima, viene analizzato utilizzando l'emulatore di sistema, che controlla l'esecuzione di tutte le istruzioni. Può individuare le tecniche di evasione avanzate che altre sandbox non rilevano. [5]

WatchGuard ha selezionato un partner best-of-breed per lo sviluppo del servizio APT Blocker: Lastline Technology che è stata fondata dal team tecnico che ha sviluppato Anubis, lo strumento utilizzato dai ricercatori di tutto il mondo negli ultimi otto anni per analizzare i file alla ricerca di potenziale malware [6].

Quando viene rilevato il malware può essere immediatamente bloccato a livello del firewall. In alcuni casi un zero-day potrebbe passare attraverso mentre l'analisi avviene nel cloud. In tale caso, il sistema di WatchGuard è in grado di fornire avvisi in pochi minuti che una parte di codice sospetto è sulla rete in modo che si possa reagire immediatamente.

Tipi di file analizzati da APT Blocker:

- Tutti gli eseguibili Windows
- Adobe PDF
- Microsoft Office
- Android Application Installer (.apk)
- Gli zip file (.zip) vengono decompressi

Visibilità

Ma il rilevamento del malware non è sufficiente. Lo staff IT ha bisogno di ottenere informazioni chiare e utili che non si perdano in un oceano di informazioni di log. Nonostante l'enorme impatto che gli incidenti di sicurezza possono avere in un'azienda, molti dipartimenti IT guardano con sospetto presunti avvisi di sicurezza. Neiman Marcus, un'altra catena di vendita al dettaglio degli Stati Uniti che è stata recentemente violata, ha avuto più di 60.000 linee di log che mostravano come vi fosse un malware sul loro network. [7] Target aveva avuto log evidenti a partire da un paio di giorni dopo la prima violazione che indicavano un problema evidente ma furono ignorati. [8]

Qualsiasi soluzione di rilevazione del malware avanzato deve comportarsi in questo modo:

- Inviare **allarmi via Email** quando viene rilevato un file dannoso
- **Log e le capacità di report** devono essere strettamente integrate con altre funzionalità di sicurezza sulla rete

- Fornire una **chiara indicazione del motivo** per cui un file è stato rilevato come malware, quindi non venire immediatamente liquidato come un potenziale falso positivo

La soluzione APT Blocker WatchGuard soddisfa tutti i requisiti di visibilità con avvisi e-mail, analisi dei log in tempo reale e la capacità di andare più in profondità per trovare maggiori informazioni. Il servizio è completamente integrato nel WatchGuard Dimension, Il pluripremiato sistema di visibilità [9] e di analisi intelligente dei log inclusa gratuitamente con tutte le soluzioni UTM di WatchGuard. Si va quindi al di là di un semplice avviso riguardo un file sospetto, e viene fornito un rapporto dettagliato delle attività dannose per ogni file che viene ritenuto un malware.

Figura 4: Report APT che mostra i dettagli di Malicious Activity con la spiegazione del perché un file viene contrassegnato come malware

L'esempio precedente evidenzia un file che mostra diverse caratteristiche che sono tipiche di un malware. Le due evasioni dimostrano come la soluzione è stata in grado di rilevare attività dannose che possono aver ingannato altre soluzioni sandbox.

WatchGuard Dimension rende trasparenti le attività di sicurezza di rete, come quelle catturati da APT Blocker, e consente agli amministratori di andare più a fondo alla ricerca di dati più dettagliati.

Dimension include più di 70 rapporti completi, con la possibilità di pre-pianificare i report per il recapito via posta elettronica. Le opzioni includono report di riepilogo, di dettaglio e speciali conformi a HIPAA e PCI. L'Executive Report è una sintesi di alto livello su misura per responsabili IT, responsabili della conformità e proprietari di piccole imprese.

Sommario: Tenete al sicuro i dati con la Advanced Malware Detection

Le minacce si sono evolute. Gli hacker utilizzano verso le aziende le stesse tecniche avanzate che in precedenza erano utilizzati durante attacchi contro gli Stati nazionali.

Soluzioni di sicurezza devono evolvere per stare al passo con queste minacce e per mantenere la rete sicura. Il rilevamento del malware basato su firme non è più sufficiente. Antivirus e Intrusion Prevention System sono ancora una parte necessaria nella difesa di qualsiasi azienda, ma hanno bisogno di essere integrate con nuove funzionalità di rilevamento avanzate con quattro caratteristiche chiave.

1. **Sandbox nel cloud** con l'emulazione completa del sistema - con la capacità di analizzare diversi tipi di file
2. **La capacità di andare oltre la sandbox** per individuare diverse forme di evasioni avanzate.
3. **Visibilità in modo che il personale che opera sulla rete** e il team IT ricevano avvisi chiari di tutti i malware e le spiegazioni del perché ciascun file rilevato è considerato dannoso.
4. **Non solo rilevamento**, ma la capacità di prendere in modo proattivo l'azione e bloccare i file pericolosi.

WatchGuard Blocker APT va oltre la rilevazione antivirus signature-based, utilizzando un sandbox cloud-based con l'emulazione completa del sistema per rilevare e bloccare il malware avanzato e gli attacchi zero day.

Per ulteriori informazioni su WatchGuard Blocker APT, visitare il sito www.watchguard.com/apt

Note:

[1] http://en.wikipedia.org/wiki/SQL_Slammer

[2] http://watchguardsecuritycenter.com

[3] http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/

[4] http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/

[5] http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware

[6] http://info.lastline.com/blog/different-sandboxing-techniques-to-detect-advanced-malware

[7] http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[8] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

[9] http://www.watchguard.com/news/press-releases/network-computing-awards-names-watchguard-dimension-best-new-product-of-the-year.asp

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.