Bitdefender®

Rapporto sul panorama mondiale delle minacce elettroniche - 2017

Introduzione

Negli ultimi mesi abbiamo assistito a una notevole ridefinizione del panorama delle minacce. Minacce tradizionali, come Trojan, ransomware e spam bot generici, sono state integrate drasticamente da distruttori di dati. Potenziati da codice di livello militare presumibilmente sottratto alla NSA, sia WannaCry che GoldenEye hanno provocato molti danni tra il secondo e il terzo trimestre di quest'anno, bloccando intere aziende e causando perdite operative senza precedenti.

Nuovi vettori di movimento laterale hanno integrato exploit zero-day come EternalBlue ed EternalRomance per conquistare gli spazi aziendali. Altre tendenze significative nel 2017 sono state il maggior interesse a strumenti open-source o freeware riuniti da un codice personalizzato per creare vere e proprie armi in grado di supportare i piani degli aggressori.

Le nostre indagini su APT e attacchi mirati nel 2017 hanno svelato strumenti gratuiti come utility di recupero della password di Nirsoft e programmi di cifratura legittimi, come DisckCryptor e simili, che hanno reso la rilevazione e la risoluzione sempre più difficili.

Questi attacchi mirati stanno rimodellando il panorama della sicurezza aziendale o governativa, causando forti ricadute nello spazio dei consumatori, in quanto i pirati informatici si stanno impegnando nell'adottare exploit noti e tecnologie di movimento laterale avanzate nei propri payload.

Bitdefender sta monitorando costantemente la sua rete globale di oltre 500 milioni di sensori e honeypot per rilevare eventuali minacce emergenti o attacchi informatici minori, che cercano di superare i controlli dei prodotti di sicurezza. I dati aggregati ci consentono di rappresentare un quadro piuttosto accurato di ciò che sta accadendo nel settore, aiutandoci a sviluppare nuovi rimedi per la prossima generazione di minacce informatiche.

Questo rapporto si basa esclusivamente sulle informazioni ottenute tramite una vasta gamma di servizi di sicurezza in Gravityzone: Security for Virtualized Environments, Security for Endpoints, Security for Mobile e Security for Exchange, prodotti per utenti finali, come Bitdefender Antivirus, Bitdefender Internet Security o Bitdefender Total Security, oltre a Bitdefender BOX, l'innovativa soluzione per proteggere i dispositivi nel proprio spazio IoT.

Osservazioni principali

I dati di Bitdefender mostrano che i ransomware sono ancora la minaccia più frequente. Solo nel corso del 2017, il numero di nuove famiglie principali di ransomware ha superato le 160, con decine o persino centinaia di variazioni per famiglia. Il ceppo di ransomware più prolifico è Troldesh / Crysis, con centinaia di sottovarianti finora esistenti. GlobeImposter, un'altra famiglia di ransomware estremamente prolifica, compete testa a testa con Troldesh nel numero di sottovarianti rilasciate.

L'ecosistema dei malware commerciali è concentrato soprattutto nel sviluppare e piazzare i ransomware. Le nostre statistiche mostrano che **un messaggio e-mail di spam su sei è dotato anche di una qualche forma di ransomware** (link a siti di download drive-by, allegati dotati di ransomware o persino downloader JavaScript/VBS per ransomware).

Un altro sviluppo spettacolare nel panorama delle minacce del 2017 è la **ricomparsa di Qbot** (anche conosciuto come Brresmon o Emotet), un worm multiuso e network-aware con capacità di backdoor, che circola ormai da diversi anni. È ricomparso con una significativa riprogettazione dell'infrastruttura di comando e controllo e, soprattutto, con un motore polimorfico cloud-based che gli consente di assumere virtualmente un numero illimitato di forme per evitare la rilevazione degli AV.

I ransomware destinati appositamente alle aziende ormai sono una realtà. Vista la ricomparsa lo scorso marzo della famiglia di ransomware Troldesh, le aziende hanno dovuto affrontare attacchi estremamente mirati che sfruttavano il Remote Desktop Protocol per connettersi all'infrastruttura, infettando manualmente i computer. Ransomware come Troldesh e GlobeImposter hanno strumenti di movimento laterale (come Mimikatz) per infettare le aziende e meccanismi di rimozione di registri per coprire le proprie tracce.

I miner di criptovalute hanno assunto più forme e approcci nel 2017. I classici miner illegali si sono precipitati ad adottare tattiche di movimento laterale, come gli exploit EternalBlue ed EternalRomance, presumibilmente originati dalla NSA, per infettare i computer aziendali e aumentare gli sforzi di mining. Il rappresentante di questa categoria è il miner di Monero, Adylkuzz, che è comparso ai primi di maggio, circa nello stesso periodo di WannaCry. Un altro sviluppo rilevante da parte degli aggressori è stata l'inserimento di codice di mining in siti web compromessi per raggiungere un pubblico più ampio e aumentare la resa del mining stesso.

[2]

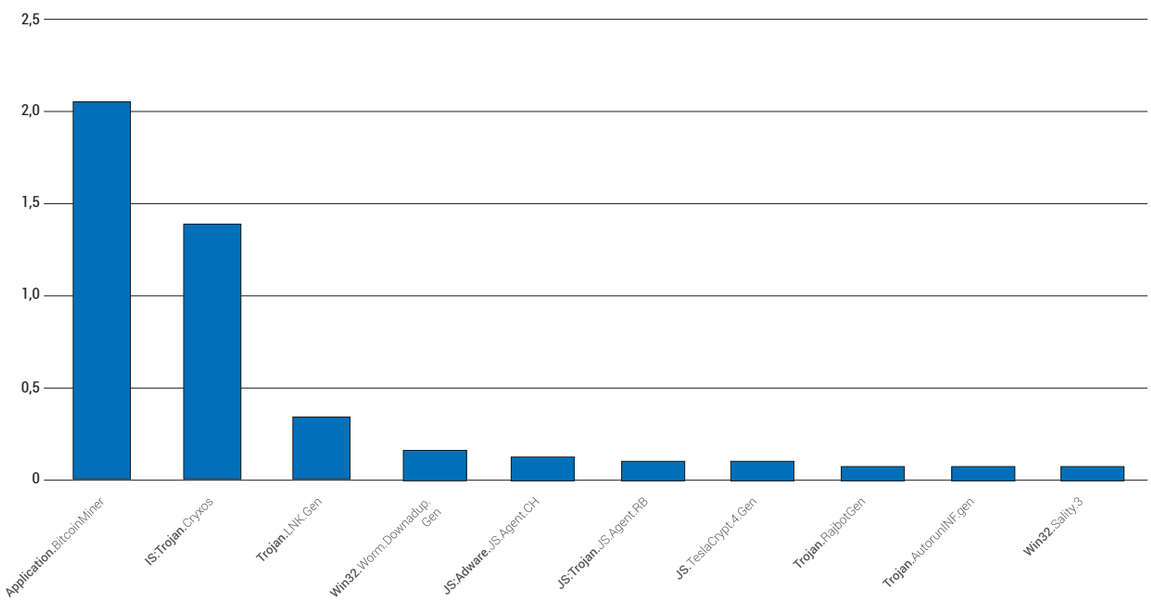
Uno sguardo al panorama delle minacce di Windows

Le informazioni sulle minacce di Bitdefender mostrano che gli Stati Uniti sono ancora la destinazione preferita per i crimini informatici. Gli Stati Uniti sono al primo posto come numero di incidenti dannosi rilevati nel corso del 2017 con il 18,5% degli incidenti rilevati proprio dai sensori di Bitdefender.

I miner di Bitcoin illeciti dominano il vertice delle classifiche di quest'anno, contando per oltre l'1,05% di tutte le infezioni rilevate a livello mondiale. Application.BitdcoinMiner è il principale rappresentate di questa categoria e consiste in un miner legittimo, configurato per violare gli sforzi di mining per vari portafogli. L'applicazione, insieme al suo file di configurazione, viene inserita furtivamente nei computer delle vittime.

JS:Trojan.Cryxos è un altro interessante protagonista del rapporto sulle minacce del 2017. Questa rilevazione riguarda codice JavaScript associata a siti web hackerati per mostrare finestre a comparsa allarmanti. Questi Trojan fanno parte di truffe del tipo "chiama il supporto" o un finto "supporto tecnico", in cui siti web compromessi mostrano anche un numero di un servizio di supporto ospitato però da pirati informatici che offrono "assistenza" a pagamento. Globalmente, gli account del Trojan Cryxos raggiungono l'1,39% di tutte le segnalazioni di malware.

Epidemie di malware per nome rilevato (l'asse Y rappresenta le percentuali)



In terza posizione nelle classifiche malware del 2017 c'è una minaccia più datata chiamata Trojan.LNK. Tale rilevazione in realtà è basata su più famiglie di malware che utilizzano file di scelta rapida modificati con un'estensione .LNK, progettata per ingannare gli utenti a lanciare file dannosi.

Il quarto posto è occupato dal worm Downadup, che è tuttora attivo su computer privi di patch. Per quasi 10 anni, il worm Downadup è stata una presenza costante al vertice della classifica e continua a diffondersi, creando attività programmate sui computer infetti.

Il quinto e il sesto posto sono occupati rispettivamente dalle famiglie JS:AdwareJS.Agent e JS:TrojanJS.Agent, due veri grandi categorie di Trojan utilizzati per diversi scopi.

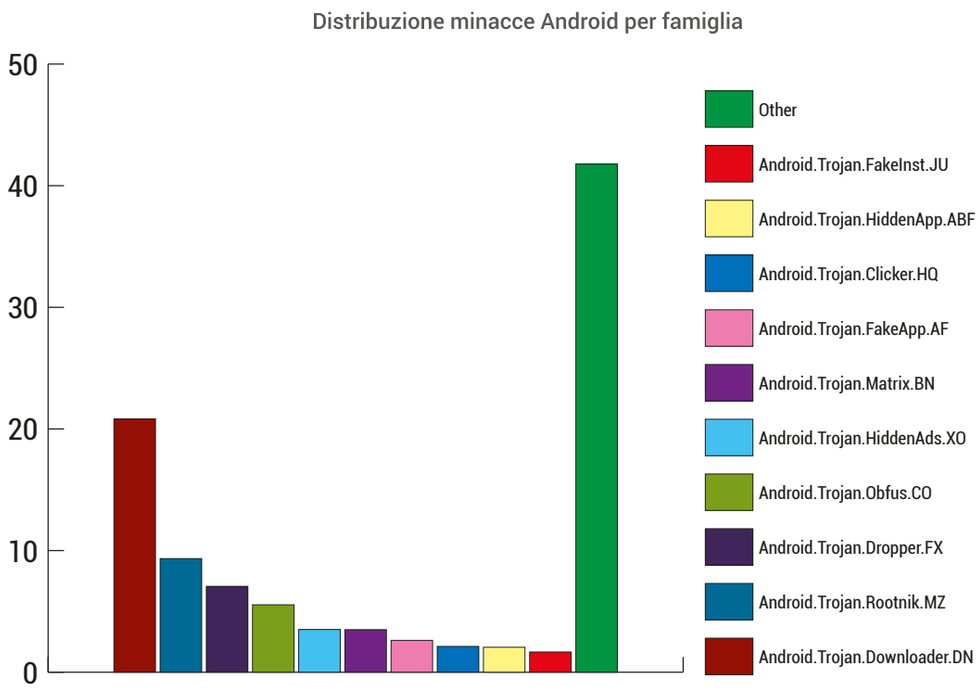
Al settimo posto, JS.TeslaCrypt4 è un downloader generico che porta l'eseguibile di TeslaCrypt sul computer delle vittime. Questa minaccia viene distribuita tramite e-mail e agisce da downloader di prima fase che recupera ed esegue il payload di TeslaCrypt.

Trojan.Rajbot si classifica ottavo nella top 10 2017 dei malware. Questo tipo di malware multifunzionale è scritto in Node.JS. È dotato del suo interprete JavaScript che gli consente di essere eseguito esternamente a un browser e include un'architettura plug-and-play, che permette il suo riutilizzo in diversi scenari.

Classificandosi nono nella classifica delle maggiori minacce malware del 2017, AutorunInf è ancora attivo e associato allo 0,7% delle segnalazioni di malware globali. Anche se i suoi meccanismi di diffusione non funzionano più sui sistemi operativi moderni, i file dannosi in esecuzione automatica vengono ancora rilevati sui supporti rimovibili che sono entrati in contatto con i computer infetti con Windows XP.

Win32.Sality conclude la nostra classifica dei malware, con lo 0,66% di infezioni in tutto il mondo. Questo iniettore di file polimorfico è operativo da anni. Infetta i file eseguibili su supporti di archiviazione locali o rimuovibili, e inserisce il computer infetto in una rete peer-to-peer di macchine compromesse, dove attende ulteriori istruzioni.

Analisi delle minacce per Android



Android. Trojan.Downloader.DN	**20,82%**
Android. Trojan.Rootnik.MZ	**9,34%**
Android. Trojan.Dropper.FX	**7,06%**
Android. Trojan.Obfus.CO	**5,54%**
Android. Trojan.HiddenAds.XO	**3,51%**
Android. Trojan.Matrix.BN	**3,50%**
Android. Trojan.FakeApp.AF	**2,62%**
Android. Trojan.Clicker.HQ	**2,12%**
Android. Trojan.HiddenApp.ABF	**2,05%**
Android. Trojan.FakeInst.JU	**1,66%**
Altro	**41,78%**

Una delle famiglie di malware Android prevalenti sembra essere Android.Trojan.Downloader, che occupa il primo posto con il 20,82% di tutte le segnalazioni. Questa famiglia è nota per ingannare le vittime facendogli scaricare diversi tipi di finte applicazioni, spacciandosi per aggiornamenti legittimi di Flash e Adobe. Generalmente distribuita tramite siti o pagine web compromesse, con contenuti per adulti,

questa famiglia di malware è utilizzata soprattutto per distribuire malware con una vasta gamma di funzionalità.

La seconda famiglia di malware Android più diffusa è Android.Trojan.Rootnik (9,34%), nota soprattutto per utilizzare una vasta gamma di strumenti di rooting commerciali per ottenere accesso come root in dispositivi infettati. Il suo obiettivo è sottrarre informazioni e scaricare ulteriori app (dannose) per dare agli aggressori un appiglio permanente e il pieno controllo del dispositivo Android compromesso. Considerando che alcuni campioni di questa famiglia di malware sono in grado di sfruttare diversi exploit di root, è molto versatile ed efficace nelle mani dei pirati informatici.

Un'altra famiglia di malware Android piuttosto diffusa è Android.Trojan.Dropper (7,06%), destinata a controllare il dispositivo infetto e renderlo parte di una botnet, contro gli altri. Alcune varianti di questa famiglia hanno diverse abilità, tra cui capacità simili a Trojan, come accedere e sottrarre dati o consentire l'accesso remoto a pirati informatici.

Un altro Trojan per Android con capacità di raccolta dati è la famiglia Android.Trojan.Obfus (5,54%), che in alcuni casi può anche rilevare i tasti utilizzati sulla tastiera o inviare e scaricare file da un server di comando e controllo (C&C). Non limitandosi solo a tali "caratteristiche", questa particolare famiglia di malware ha campioni che includono diverse funzionalità malware.

Anche gli adware Android sono abbastanza comuni, in particolare, due famiglie, Android.Trojan.HiddenAds (3,51%) e Android.Trojan.HiddenApp (2,05%) sono note per mostrare una moltitudine di pubblicità, una volta installati sui dispositivi delle vittime. I pirati informatici spesso riconfezionano applicazioni legittime con queste famiglie di malware aggressive per far cliccare gli utenti sul maggior numero di pubblicità possibile, generando quindi dei ricavi che incasseranno. Sebbene non dannose in quanto tali, queste applicazioni riconfezionate possono rallentare seriamente le prestazioni di un dispositivo, mostrare schermate fastidiose e danneggiare l'esperienza utente generale.

La famiglia di malware Android.Trojan.Matrix (3,5%) è piuttosto nota e normalmente viene utilizzata sia per accedere a un dispositivo, così da consentirne il controllo remoto, sia per avvisare continuamente gli utenti di installare applicazioni dannose aggiuntive con capacità di adware o funzioni più pericolose. Distribuita generalmente tramite finte applicazioni che si presentano come programmi per lo streaming di video per adulti, questa famiglia di malware normalmente punta alle versioni più datate di Android.

Android.Trojan.FakeApp (2,62%) e Android.Trojan.FakeInst (1,66%) sono due famiglie di malware Android distribuite generalmente tramite alcune popolari app per Android manomesse o false. Il loro scopo principale è mostrare pubblicità, ottenere informazioni personali dai dispositivi infettati e persino inviare messaggi di testo a numeri con tariffazione molto elevata. Alcune variante di Android.Trojan.FakeInst sono note per fingere persino di essere soluzioni di sicurezza, in genere allertando gli utenti a installarle rapidamente per risolvere alcuni finti problemi di sicurezza.

Anche se probabilmente non è così popolare come le altre famiglie di malware, la famiglia Android.Trojan.Clicker (2,12%) viene comunemente utilizzata per reindirizzare gli utenti a siti web controllati dall'aggressore e incrementare il traffico in maniera illegittima o invitare gli utenti a installare app dannose. Alcune varianti possono persino consentire agli aggressori di trasformare i dispositivi infetti in bot e utilizzarli per eseguire attacchi DDos contro determinate vittime.

Che cosa ci aspetta

Mentre il 2017 volge al termine, l'unità di analisi delle minacce di Bitdefender sta attualmente analizzando gli sviluppi dei prossimi malware, che cercheranno di emergere nell'anno ormai in arrivo. Gli esperti di Bitdefender prevedono un aumento degli exploit zero-day trapelati dalle agenzie di sicurezza di tutto il mondo e importanti cambiamenti nel modo di operare da parte dei ransomware.

Dopo essersi concentrati per anni soprattutto sui singoli utenti, gli autori di malware colpiranno sempre più aziende e reti di computer. Il movimento laterale diventerà standard nella maggior parte dei campioni di malware, sia tramite utility di ottenimento delle password, come Mimikatz, sia sfruttando vulnerabilità tramite worm.

Il numero di allegati dannosi nelle e-mail di SPAM aumenterà, in particolare per quelle scritte in linguaggi di programmazione, come PERL o Python. Anche gli attacchi privi di file aumenteranno sensibilmente mentre l'adozione di Windows 10 diventerà universale, sfruttando il supporto della piattaforma di Powershell o Linux Bash.

Il panorama delle minacce resterà fedele ai malware che monetizzano meglio: ransomware, Trojan bancari e miner per valuta digitale, ma queste minacce andranno incontro a profondi cambiamenti nel modo in cui operano. Ci attendiamo di vedere ransomware in grado di sfruttare la potenza della GPU per agire più rapidamente e tentare di superare i prodotti antimalware.

Gli esperti Bitdefender si attendono anche grandi cambiamenti nel mercato PaaS (polimorfismo come servizio), una tendenza che si consoliderà nel corso del 2018. I motori polimorfici avanzati in esecuzione nel cloud sono già stati utilizzati dai pirati informatici per inondare il mercato di varianti uniche di malware noti e i vantaggi che gli offrono sono straordinari. L'accesso su licenza a questi motori

personalizzati genererà probabilmente ottimi affari a tali soggetti.

Tali motori poliformici saranno integrati anche con algoritmi di apprendimento automatico sfruttati in maniera negativa. Nel 2018, ci attendiamo di vedere maggiori sforzi sulle tecniche per opporsi all'apprendimento automatico, che avanzeranno principalmente in due direzioni: creando e diffondendo campioni che faranno generare ai fornitori di sicurezza falsi positivi o manipolando il payload finché non diviene inosservato.

Nel 2018, le principali minacce cercheranno anche vulnerabilità nei componenti che risiedono sotto il sistema operativo, come i firmware. Gli stack Wi-Fi e Bluetooth otterranno maggiore attenzione, in quanto le potenziali vulnerabilità identificate a tale livello offrono una backdoor furtiva by design molto difficile da rilevare e mitigare.

Le grandi botnet di IoT diventeranno normali nel 2018. Il codice sorgente per bot IoT è già disponibile gratuitamente su Internet e i gruppi di pirati informatici interessati a compromettere i dispositivi IoT hanno già una solida piattaforma per personalizzare le proprie esigenze. Prevediamo che questo codice sarà migliorato nel 2018 per consentire il movimento laterale nella rete compromessa in modo da inviare ransomware o spam.

Ultimo ma non meno importante, ci attendiamo una maggiore attività per quanto riguarda lo spazio dedicato a OS X. Per i consumatori, i malware probabilmente si concentreranno sulle tattiche scareware per costringere le vittime a pagare per strumenti inutili. Le aziende assisteranno probabilmente a più attacchi mirati, oltre a payload dannosi utilizzati in minacce persistenti avanzate.

Bitdefender Hypervisor Introspection è una delle prime soluzioni di sicurezza di questo tipo ed è stata ottenuta tramite una collaborazione unica con Citrix. Si inserisce nelle Direct Inspect API uniche di XenServer per ottenere una panoramica sulle macchine che protegge, non inserendo alcun agente in esse. Ciò rende Hypervisor Introspection immune agli attacchi, senza rischiare compromissioni dalle minacce a livello di kernel. Un vero livello di sicurezza senza agente, che proteggerà persino gli altri livelli di sicurezza, come quella per endpoint, impedendo che venga compromesso dagli aggressori. Bitdefender Hypervisor Introspection funziona oltre i livelli di sicurezza esistenti ed è compatibile con ogni altro fornitore di sicurezza.

I clienti di Bitdefender che non usano Hypervisor Introspection erano comunque protetti dall'epidemia.

Le soluzioni di GravityZone Endpoint Security hanno impedito l'esecuzione di tutte le varianti di ransomware, sfruttando i loro modelli di apprendimento automatico, che sono stati sviluppati appositamente per rilevare attacchi ransomware inediti nella fase di pre-esecuzione. In questo attacco specifico, un modello di apprendimento automatico a livello di endpoint, sviluppato dai laboratori di Bitdefender nel 2013, è stato in grado di rilevare e bloccare tutte le varianti usate dal ransomware WannaCry.

Le tecnologie di apprendimento automatico e introspezione della memoria di nuova generazione Bitdefender hanno permesso ad aziende di tutto il mondo di restare al sicuro dal mega attacco di WannaCry e dal relativo exploit zero-day EternalBlue, e garantiranno una simile protezione dai prossimi attacchi analoghi.

Per ulteriori informazioni su Bitdefender Hypervisor Introspection, visitare la pagina www.bitdefender.it/hvi

Per maggiori informazioni sulla linea di prodotti di sicurezza di Bitdefender, visitare www.bitdefender.it/business.

BD-Business-Nov.13.2017-ITk#:CREA2186
Bitdefender-Business-2017-Whitepaper-threat_landscape-crea2186-it_IT