Emotet fa strage in Germania. Francoforte bloccata per 24 ore

Dic 20, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Una serie di attacchi mirati ha colpito numerosi enti pubblici, obbligando gli amministratori a bloccare tutti i sistemi per impedire maggiori danni.

È in circolazione da più di cinque anni, ma continua a rappresentare una minaccia straordinaria per aziende ed enti pubblici in tutto il mondo. Stiamo parlando di **Emotet**, il trojan che nell'ultima settimana ha devastato le infrastrutture IT di mezza Germania.

A subire i maggiori danni è stata la municipalità di **Francoforte**, che ha dovuto forzare uno shutdown di tutti i sistemi IT per bloccare la propagazione del malware all'interno delle infrastrutture informatiche. **Un blocco di 24 ore che ha messo K.O. tutti i siti Internet e i servizi online per i cittadini**.

Secondo quanto riportano fonti di stampa locali, l'infezione sarebbe partita da una semplice email. Dal PC compromesso, il trojan avrebbe poi cominciato a diffondersi attraverso la rete locale.

La procedura di blocco di ogni attività informatica è stata giustificata con il timore (fondato) che l'attacco potesse avere conseguenze ulteriori, come l'installazione di un **ransomware** che avrebbe potuto provocare ancora maggiori danni.

Una scelta dettata, probabilmente, dall'esperienza e dalla conoscenza del **modus operandi** dei pirati, che nell'autunno del 2018 avevano colpito gli Stati Uniti all'indomani dell'emergenza provocata dall'uragano Florence, utilizzando Emotet per distribuire un ransomware sui computer compromessi.

Oltre a Francoforte, in Germania Emotet ha colpito nelle ultime due settimane anche l'Università Justus Liebig di **Gießen**, la municipalità di **Bad Homburg** e l'Università Cattolica di **Friburgo**.

Gli episodi, che hanno corrispettivi anche in altre parti del mondo, non arrivano però inaspettati. **Negli scorsi mesi, infatti, si erano susseguiti una serie di indizi che lasciavano pensare a una recrudescenza degli attacchi portati con Emotet**.

Il malware, comparso nel 2014, si è evoluto con il tempo adottando una struttura modulare che lo rende ancora più versatile e pericoloso.

Recentemente gli esperti di sicurezza hanno lanciato l’allarme su una possibile ondata di attacchi, segnalando che nell’ottobre del 2018 la botnet aveva dato segnali di attività anomala che non faceva prevedere nulla di buono.

Ulteriori segnali di un possibile ritorno “in grande stile” erano arrivati poi quest’estate, quando i ricercatori di **Malware Tech** avevano segnalato una ripresa di attività da parte dei server Command and Control utilizzati dal gruppo di pirati informatici legati a Emotet.

Condividi l’articolo

Il SIEM cresce e sfocia in altri servizi

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/20/emotet-fa-strage-in-germania-francoforte-bloccata-per-24-ore/

Il SIEM cresce e sfocia in altri servizi

Dic 19, 2019 Giancarlo Calzetta Approfondimenti, In evidenza, RSS, Software 1

Sviluppare un SIEM efficace al giorno d’oggi significa mettere le mani in pasta in moltissimi aspetti della sicurezza e questo permette di creare nuovi servizi.

I software SIEM sono da sempre degli ottimi alleati dei responsabili della sicurezza. Considerato quanti prodotti bisogna inserire nella infrastruttura per proteggere utenti e dati da **una quantità di minacce sempre maggiore**, al giorno d’oggi non può mancare un aiuto nella gestione degli eventi e delle segnalazioni che arrivano da decine di console diverse.

“Per questo” – dice Massimo Turchetto, CEO e fondatore di SGbox – “le aziende apprezzano sempre di più i SIEM, soprattutto dalle medie dimensioni in su”. In effetti, tutti gli strati che compongono la difesa di un’azienda moderna generano una **quantità di allarmi ingestibile** per un team “umano” senza un aiuto tecnologico concreto.

SGBox sviluppa SIEM in Italia da sette anni e il suo prodotto si è sempre distinto per performance e comodità d’uso. Oltre al classico motore di Log Management, che da sempre è alla base di questo tipo di soluzioni, la piattaforma si è sviluppata fino a garantire anche una funzione di Log Correlation, ovvero **un sistema che mettere in relazione tra loro gli eventi registrati da prodotti diversi** per scovare segni di compromissione o di attacco ed elevare il livello della segnalazione.

“A breve” – continua Turchetto – “arriverà anche un motore di analisi del comportamento degli utenti che migliorerà ulteriormente la qualità delle rilevazioni”.

Il SIEM, quindi, non è più solo un "punto di raccolta" per gli allarmi, ma **un sistema intelligente in grado di fornire un aiuto notevole** nel catalogare e gerarchizzare le investigazioni.

Un sistema che, inevitabilmente, **crea fortissime competenze in molti settori della sicurezza informatica** e che SGBox va a sfruttare tramite una offerta di servizi alle aziende che andrebbe vista come un percorso.

I primi due sono assessment, ovvero **analisi e report, rispettivamente sulle vulnerabilità e sullo stato della rete aziendale** (dispositivi presenti, appliance, connessioni e così via). Condotti tramite procedure automatizzate e operazioni manuali, forniscono la base per organizzare la vera e propria difesa, partendo da un quadro completo sul quale operare.

A seguire, è disponibile un servizio di **penetration testing** volto a verificare quanto le contromisure in essere riescano a far fronte agli attacchi. Le operazioni sono molto flessibili e si basano sulle linee guida del NIST (National Institute of Standards and Technology).

"In futuro" – conclude Turchetto – "andremo a raffinare sempre più i prodotti disponibili e a crearne di nuovi per sostenere anche la nostra crescita sul mercato estero."

Condividi l'articolo

Attenti agli insider: spesso la minaccia arriva dall'interno

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/12/19/il-siem-cresce-e-sfocia-in-altri-servizi/

Attenti agli insider: spesso la minaccia arriva dall'interno

Dic 19, 2019 Marco Schiaffino Gestione dati, In evidenza, Leaks, News, RSS, Scenario 1

Il rischio di un furto di dati provocato da "insider" continua a rappresentare un problema enorme per le aziende. E il cloud non aiuta…

Difendersi da pirati informatici e gruppi hacker è indispensabile. Spesso, però, il pericolo non arriva dall'esterno, ma si annida all'interno del perimetro aziendale.

Il tema viene messo a fuoco all'interno del **Data Exposure Report** pubblicato da **Code42** (si può scaricare previa registrazione a questo indirizzo) che raccoglie dati provenienti da oltre mille esperti di sicurezza informatica per tratteggiare il quadro di ciò che sta succedendo nelle aziende in merito alla protezione dei dati nei confronti delle minacce "interne".

La ricerca pone l'accento, in particolare, sulla contraddizione tra l'esigenza di proteggere i dati aziendali e

quella di offrire strumenti di lavoro che migliorino la produttività dei lavoratori. Il riferimento, qui, è in particolare agli strumenti basati sulle piattaforme cloud, che negli ultimi anni hanno letteralmente conquistato le aziende.

La flessibilità delle piattaforme virtuali ha migliorato le prestazioni e reso più "dinamiche" le aziende, mentre i sistemi di condivisione delle informazioni hanno permesso di aumentare la produttività degli impiegati.

Tutto questo, però, ha un rovescio della medaglia: l'adozione degli strumenti basati su tecnologie cloud ha infatti provocato un aumento esponenziale del rischio di data breach a livello aziendale.

I dati viaggiano infatti a una velocità impressionante e possono essere condivisi con (eccessiva) facilità attraverso una moltitudine di canali diversi. **Risultato: tenere traccia di ciò che viene condiviso diventa praticamente impossibile**.

Sul campione di aziende analizzato, il 38% ha subito una violazione dei dati nel corso degli ultimi 18 mesi e la metà di questi riportano che l'attività degli impiegati è stata in qualche modo una delle cause dell'incidente.

I problemi sono numerosi, a partire dall'uso diffuso di servizi di condivisione come **Google Drive** o **Microsoft OneDrive** attraverso account personali dei dipendenti, che per loro natura non sono sottoposti ai controlli e alle policy

dell’azienda.

C’è poi la possibilità che la violazione dei dati avvenga a causa di un atto deliberato. Il caso più frequente è quello degli impiegati che si licenziano (o vengono licenziati) portando sul nuovo posto di lavoro informazioni cui hanno accesso grazie ai sistemi di condivisione che utilizzavano all’interno dell’azienda.

Il sondaggio eseguito da Code42, in questo caso, è piuttosto illuminante: **il 59% degli intervistati ha infatti ammesso di aver “introdotto” nell’azienda in cui lavorano idee, informazioni o progetti che avevano sviluppato per un precedente datore di lavoro**.

Niente di nuovo, sia chiaro, ma se un tempo un’azienda avrebbe potuto insospettirsi nel vedere un impiegato che abbandona il posto di lavoro andarsene con 10 faldoni di documenti cartacei, oggi dovrebbe porsi il problema di verificare quali dati conservi nel suo archivio cloud.

Condividi l’articolo

Il SIEM cresce e sfocia in altri servizi Gangnam Industrial Style: attacchi a centinaia di aziende

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/12/19/attenti-agli-insider-spesso-la-minaccia-arriva-dallinterno/

Gangnam Industrial Style: attacchi a centinaia di aziende

Dic 18, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 0

Il gruppo di pirati informatici ha preso di mira in particolare le aziende del settore industriale con sede in Corea del Sud.

Una vera e propria campagna che sta coinvolgendo centinaia di società in mezzo mondo e che avrebbe l'obiettivo di rubare informazioni sensibili e segreti industriali.

A svelare le tattiche dei pirati informatici che operano la **Gangnam Industrial Style** sono i ricercatori di **CyberX**, che hanno pubblicato un report che riassume le modalità di attacco e offre una panoramica sulle aziende colpite.

I cyber-criminali, spiegano i ricercatori, utilizzano una

variante di un vecchio malware chiamato **Separ**, individuato per la prima volta nel 2013. La nuova versione contiene una serie di funzionalità aggiuntive rispetto all'esemplare individuato 6 anni fa.

In particolare, notano dalle parti di CyberX, questa versione è programmata per rubare, oltre alle password, anche **tutti i file che corrispondono a determinate estensioni** (documenti di office e immagini) e integra un sistema che sfrutta la funzione di Autorun per garantirsi persistenza sulla macchina infetta.

Ciò che rende particolarmente insidioso l'attacco, però, non sono tanto le caratteristiche del trojan, quanto la cura con cui i pirati informatici hanno pianificato questa colossale campagna di attacchi.

I bersagli, scelti con cura tra le aziende che operano nel settore industriale, sono per la maggior parte (circa il 60%) società con sede nella **Corea del Sud**, ma tra le vittime ci sono anche aziende che operano in **Cina, Tailandia, Ecuador, Regno Unito e Germania**.

Il vettore di attacco è rappresentato da email che vengono confezionate su misura per ogni bersaglio e che sono camuffate in modo da sembrare comunicazioni legittime da parte di enti pubblici o altre aziende, con riferimenti specifici a progetti realmente esistenti.

I messaggi di posta elettronica vengono corredati da numerosi allegati. **In uno dei casi analizzati dal team di ricercatori, al messaggio era allegata anche della documentazione estremamente credibile relativa a un sistema commercializzato da Siemens**.

Il malware, invece, è nascosto all’interno di un archivio compresso in formato ZIP che, una volta aperto, appare contenere dei semplici PDF.

In realtà i file sono degli eseguibili (i pirati ne hanno alterato l’icona) che, una volta avviati, eseguono una serie di operazioni tra cui la disattivazione di **Windows Firewall**, la copia delle password del browser e del programma di posta elettronica, delle email stesse e dei file di potenziale interesse. **Il tutto viene poi caricato su un server controllato dai pirati informatici attraverso un collegamento FTP**.

Stando a quanto riporta CyberX, la tecnica ha avuto un’incredibile efficacia. Le aziende compromesse dagli attacchi sarebbero infatti più di 200.

Condividi l’articolo

IoT e certificati di sicurezza: bastano 3.000 dollari per violarne 435.000

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/12/18/gangnam-industrial-style-attacchi-a-centinaia-di-aziende/

IoT e certificati di sicurezza: bastano 3.000 dollari per violarne 435.000

Dic 17, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità delle chiavi RSA individuata da un gruppo di ricercatori. Se si ha a disposizione abbastanza potenza di calcolo si possono violare.

Ancora IoT e ancora problemi di sicurezza. Il nuovo allarme relativo alla **Internet of Things** arriva da un gruppo di ricercatori di **Keyfactor**, che hanno messo sotto la lente d'ingrandimento le procedure usate dai dispositivi "intelligenti" per creare le **chiavi RSA** utilizzate nei certificati digitali.

Come si legge nel report pubblicato da Keyfactor, la ricerca ha preso in esame **75 milioni di certificati RSA** "rastrellati" su Internet e ha evidenziato lo scarso livello di qualità delle chiavi utilizzate.

I ricercatori, per la loro indagine, hanno preso le mosse da una tecnica di attacco già conosciuta, che permette di scardinare il sistema di crittografia a chiave asimmetrica RSA. La tecnica fa leva sulle modalità con cui vengono generate le chiavi.

RSA, infatti, prevede l'utilizzo di due fattori (nella pratica due numeri primi scelti casualmente) per la creazione delle chiavi. La tecnica di attacco, basata sull'analisi di grandi quantità di chiavi, permette di compromettere quelle che hanno fattori in comune.

Normalmente, spiegano i ricercatori, questa corrispondenza è piuttosto rara. In un esempio citato nel report e basato sull'analisi dei log di **Certificate Transparency**, si verifica in 5 casi su 100 milioni di sample. **La loro indagine, però, ha trovato una corrispondenza ogni 172 certificati**.

Tradotto sul campione da loro analizzato, si traduce in **435.000 certificati "deboli"**, che possono cioè essere compromessi. Per farlo, spiegano dalle parti di Keyfactor, è stato sufficiente utilizzare un server su piattaforma **Microsoft Azure** per elaborare il database di certificati. Costo dell'operazione: 3.000 dollari.

Ma cosa c’entrano i dispositivi IoT con tutto questo? Secondo i ricercatori, la diffusione dei dispositivi “smart” rende più facile l’attacco per due motivi. Prima di tutto perché la presenza dei device IoT incrementa esponenzialmente il numero di certificati in circolazione su Internet.

In secondo luogo perché i dispositivi stessi, spesso estremamente semplici, utilizzano tecniche di randomizzazione di bassa qualità, rendendo più probabile la corrispondenza dei fattori utilizzati in altre chiavi.

Lo scenario che dipingono gli autori della ricerca, se non catastrofico, è per lo meno preoccupante. La violazione dei certificati, infatti, consentirebbe di scardinare i sistemi di protezione nelle comunicazioni e, di conseguenza, portare attacchi estremamente dannosi.

Il fatto che i dispositivi IoT in questione siano utilizzati anche in ambiti industriali e nel settore automobilistico, aprono poi la strada a forme di sabotaggio estremamente pericolose.

La soluzione, secondo i ricercatori è semplice: adottare sistemi di generazione delle chiavi più sicuri. Un compito non facile anche perché, come fanno notare gli autori, la distribuzione di eventuali aggiornamenti software in grado di

mitigare il rischio sui dispositivi IoT si scontra con la scarsa sensibilità dei produttori e degli stessi utenti.

Condividi l’articolo

Mozilla: autenticazione a due fattori obbligatoria per gli sviluppatori

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/17/iot-e-certificati-di-sicurezza-bastano-3-000-dollari-per-violarne-435-000/

Mozilla: autenticazione a due fattori obbligatoria per gli sviluppatori

Dic 16, 2019 Marco Schiaffino Attacchi, In evidenza, News, Phishing, RSS, Scenario, Tecnologia 0

La mossa punta a blindare gli account dei programmatori per evitare gli attacchi supply chain nei confronti delle estensioni di Firefox.

A mali estremi, estremi rimedi. Dalle parti di **Mozilla** hanno

deciso di dare un giro di vite nella gestione delle estensioni di **Firefox** prevedendo l'uso obbligatorio dell'autenticazione a due fattori per gli sviluppatori che forniscono estensioni per il popolare browser open source.

La mossa arriva dopo un periodo in cui Firefox ha subito una raffica di attacchi "indiretti" che hanno preso di mira gli account dei programmatori in un classico schema **supply chain**.

La tecnica, sempre più adottata dai cyber-criminali, prevede la compromissione dei sistemi o degli account degli sviluppatori software per inserire malware o codice malevolo nei loro prodotti. Gli esempi registrati dalla cronaca sono numerosi e hanno coinvolto, in particolare, i produttori di smartphone asiatici.

Nel settore dei browser (**Firefox** e **Chrome**) sembra però che ci sia una pressione costante e i tentativi di "inquinare" la filiera si moltiplicano in maniera esponenziale.

Il motivo è semplice: se un pirata informatico riesce a compromettere l'account di uno sviluppatore, può distribuire rapidamente un malware inserendolo in un aggiornamento per l'estensione. **Come impostazioni predefinita, infatti, Firefox prevede l'aggiornamento automatico dei componenti aggiuntivi installati sul browser**.

Una scelta condivisibile, che garantisce un maggior livello di sicurezza per chi utilizza Firefox. **Nel caso in cui si verifichi un attacco come quello descritto, però, la funzione si trasforma in un boomerang**.

Un eventuale aggiornamento distribuito da un pirata informatico, infatti, viene immediatamente distribuito su tutti i browser su cui è installato il componente aggiuntivo originale.

Oltre a consentire di colpire un gran numero di vittime con il minimo sforzo, inoltre, un attacco supply chain che prenda di mira il browser mette il cyber-criminale in una posizione di straordinario vantaggio. **Compromettere il programma di navigazione permette infatti di rubare con facilità password e credenziali, rubare cookie di autenticazione e spiare l'attività online della vittima**.

Nella maggior parte dei casi, i pirati puntano a sottrarre le credenziali di accesso agli store attraverso **campagne di phishing mirate**. Proprio per questo motivo Mozilla avrebbe deciso di rendere obbligatorio l'utilizzo del sistema di autenticazione a due fattori per tutti gli account che accedono al portale **addons.mozilla.org**.

L'obbligo partirà dal 2020 e, nelle intenzioni dell'azienda, dovrebbe rappresentare un argine al fenomeno degli attacchi supply chain.

Condividi l'articolo

Nuova tecnica ransomware: "pagateci, le multe del GDPR costano di più"

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/16/mozilla-autenticazione-a-due-fattori-obbligatoria-per-gli-sviluppatori/

Nuova tecnica ransomware: “pagateci, le multe del GDPR costano di più”

Dic 13, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario 1

La mossa è geniale: i pirati minacciano di rendere pubblici i documenti rubati innescando le sanzioni del regolamento europeo sulla protezione dei dati.

Dopo qualche anno in cui i pirati informatici sono riusciti a incassare milioni di dollari grazie agli attacchi **ransomware**, si trovano ora costretti a inventarsi qualcosa di nuovo. SI ai semplici utenti privati che le aziende, infatti, hanno cominciato a utilizzare strumenti di prevenzione e a cedere con maggiore difficoltà ai ricatti.

La trovata del un gruppo di cyber-criminali che diffonde il ransomware **Sodinokibi**, probabilmente si colloca proprio in quest’ottica.

Stando a quanto si legge in un post comparso su un forum

hacker in Russia (il contenuto è stato postato da un ricercatore di sicurezza su Twitter – ndr) uno degli elementi utilizzati per rendere il ricatto più efficace è quello di agitare il rischio di una multa ai sensi del nuovo **GDPR**.

Nel posto, uno dei portavoce del gruppo di cyber-criminali cita un attacco portato a un'azienda da una "divisione" del gruppo dedicata ad attacchi di alto profilo. **Nel testo critica le vittime che si rifiutano di pagare precisando che, in caso di mancato pagamento, avrebbero venduto le informazioni rubate o le avrebbero rese pubbliche**.

Il tema non è nuovo: la maggior parte dei pirati informatici, infatti, non si limitano a crittografare i dati sui sistemi delle vittime, ma ne fanno una copia.

La novità è che la minaccia di rendere pubblici i dati fa leva non tanto sul danno reputazionale che potrebbe subire l'azienda, quanto la possibilità che l'attacco comporti l'attivazione del meccanismo sanzionatorio previsto dal nuovo regolamento europeo sulla protezione dei dati.

La logica, in pratica, è: "se non pagate noi, vi trovate a pagare 10 volte tanto al vostro governo".

Anche se di primo acchito la cosa può far sorridere, non è

escluso che la tecnica possa avere una certa presa sulle vittime, soprattutto nel caso in cui queste ultime dovessero avere la coscienza sporca per non aver predisposto misure di sicurezza adeguate per proteggere i dati in loro possesso.

Condividi l’articolo

I pirati nord-coreani di Lazarus adesso usano malware “in affitto”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/13/nuova-tecnica-ransomware-pagateci-le-multe-del-gdpr-costano-di-piu/

I pirati nord-coreani di Lazarus adesso usano malware “in affitto”

Dic 12, 2019 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

L’utilizzo di un nuovo malware sarebbe il senale di una

strana collaborazione tra il gruppo di "hacker di stato" Lazarus e i cyber-criminali di TrickBot.

Il mondo della pirateria informatica, ormai da anni, è caratterizzato da forme di collaborazione più o meno strette tra vari gruppi di pirati informatici. Una delle poche "barriere" che vengono considerate invalicabili è quella tra "comuni" cyber-criminali e i gruppi APT, quelli cioè che agiscono per conto di **governi e servizi segreti**. Ora sembra che anche questa distinzione sia caduta.

A segnalarlo sono i ricercatori di **SentinelOne**, che in un report pubblicato sul sito della società di sicurezza spiegano di aver individuato uno stretto rapporto tra il gruppo di cyber-spionaggio **Lazarus** e i pirati informatici di **TrickBot**.

Lazarus, di cui ci è capitato di parlare più volte su **Security Info**, è il gruppo APT che gli esperti di sicurezza considerano da sempre collegato al governo della **Nord Corea** e fino a oggi la sua attività si era caratterizzata per l'utilizzo di strumenti di hacking "fatti in casa".

Secondo gli analisti di SentinelOne, però, adesso la loro attività sfrutterebbe **Anchor**, un nuovo modulo di spionaggio sviluppato dal gruppo TrickBot.

Quest'ultimo è un soggetto ben conosciuto, che fa parte però di quella "delinquenza comune" normalmente attiva in settori orientati alla raccolta di credenziali bancarie e attacchi a soggetti che operano nella finanza.

In quest’ottica, il fatto che usi la formula del **malware as a service**, cioè che affitti ad altri criminali i suoi software, non stupisce più di tanto. Tanto più che la gang è nota per fornire servizi personalizzati in base alle esigenze dei suoi clienti.

Il nuovo modulo, però, sembra pensato proprio per chi vuole guadagnare un livello di elevata persistenza sulla macchina compromessa senza dare troppo nell’occhio. **Qualcosa, cioè, che può interessare principalmente a hacker che puntano ad attacchi mirati e allo spionaggio**.

In realtà, come spiegano i ricercatori nel report, Anchor consiste di una collezione di strumenti estremamente evoluti che, molto probabilmente, sono stati pensati in origine per “clienti” interessati a colpire bersagli di alto livello del settore finanziario.

L’interessamento del gruppo Lazarus è probabilmente dovuto a una semplice intuizione: lo stesso set di strumenti può essere utilizzato per portare avanti attività di spionaggio. **Il modulo, infatti, integra sistemi per cancellare le tracce dell’attacco e per offuscare l’attività del malware che si prestano alla perfezione a questo tipo di attività**.

Insomma: è probabile che i pirati di TrickBot non avessero assolutamente idea che il loro nuovo “prodotto” avrebbe potuto suscitare l’interesse di un gruppo di hacker di stato. Considerato che il detto “pecunia non olet” si applica benissimo anche ai bassifondi del Web, la strana alleanza tra TrickBot e Lazarus non deve stupire più di tanto.

Condividi l’articolo

Progetto Blackfin: F-Secure cambia la logica dell’intelligenza artificiale

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/12/i-pirati-nord-coreani-di-lazarus-adesso-usano-malware-in-affitto/

Progetto Blackfin: F-Secure cambia la logica dell'intelligenza artificiale

Dic 11, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia 0

La società di sicurezza punta sul concetto di "Swarm AI". L'intelligenza artificiale applicata alla cyber-security diventa collettiva e distribuita.

Nel corso della sua conferenza, **Mikko Hyppönen** descrive la nuova tecnologia di intelligenza artificiale elaborata da **F-Secure** si preoccupa di spiegare che il riferimento alla cosiddetta "intelligenza dello sciame" (swarm intelligence) è una semplice metafora che evoca meglio l'idea di fondo che ha ispirato gli sviluppatori della società di sicurezza finlandese.

Il fatto che metta le mani avanti per evitare fraintendimenti, però, non sminuisce il potenziale impatto della nuova filosofia che ha illustrato nell'incontro tenutosi a Milano nella giornata di ieri.

“Fino a oggi tutte le società di sicurezza, noi compresi, hanno utilizzato l’intelligenza artificiale in maniera centralizzata” ha spiegato Hyppönen a Security Info nel corso dell’intervista. “Con il progetto Blackfin (una particolare varietà di tonno – ndr) stiamo trasformando la tecnologia AI in un sistema distribuito”.

L’idea di base è quella di replicare il comportamento di alcuni insetti o animali che, collettivamente, riescono a raggiungere obiettivi che sarebbero impossibile ottenere singolarmente.

“Se pensiamo alle formiche o alle api, così come agli stormi di uccelli o ai banchi di pesci, ci rendiamo conto di come questa forma di intelligenza collettiva consenta di mettere in campo comportamenti decisamente più complessi ed efficaci di quanto possa essere fatto individualmente” chiosa Hyppönen.

Il concetto, paradossalmente, sembra chiudere un cerchio rispetto all’evoluzione della sicurezza informatica. Se in origine la protezione era distribuita a livello di endpoint e ha subito un processo di progressiva centralizzazione con l’introduzione delle tecniche di **detect and response** basate sull’analisi affidata all’intelligenza artificiale, lo “spezzettamento” dell’AI potrebbe paradossalmente proporre una sorta di ritorno al passato.

Secondo il guru della cyber-security, però, questa evoluzione rappresenta un futuro quasi inevitabile, che avrà un impatto

pratico notevole.

“L’utilizzo di analisi basate sull’AI a livello centralizzato è stato dettato da diverse esigenze” spiega Hyppönen. “Oltre a quella di migliorare le capacità di rilevamento, c’era per esempio quella di poter sfruttare database per il riconoscimento dei malware che avevano raggiunto dimensioni tali da non poter essere gestito a livello di endpoint”.

Questa architettura, però, comporta degli svantaggi. **La sua efficacia dipende infatti dal fatto che la singola macchina o dispositivo abbia la possibilità di comunicare costantemente con l’infrastruttura centrale**.

“Questo non può accadere sempre” puntualizza Hyppönen. “Sia per cause esogene, come nel caso delle infrastrutture IT a livello militare che non possono ovviamente prevedere canali di comunicazione esterni, sia nel caso in cui gli attaccanti adottino una strategia che gli consenta di tagliare fuori i loro bersagli dalla rete di comunicazione”.

L’utilizzo di agent indipendenti basati sull’intelligenza artificiale, insomma, permetterebbe di garantire un livello di protezione avanzato anche in situazioni che potremmo considerare “al limite”.

Ma anche in condizioni normali, l'impostazione di Blackfin offre indiscutibili vantaggi. L'analisi di un agent AI a livello locale permette infatti di eseguire un controllo molto più granulare e "tarato" sull'ecosistema in cui è stato implementato.

"Stiamo sperimentando questa tecnologia da solo tre settimane, ma abbiamo già notato alcuni vantaggi legati al suo utilizzo" spiega Hyppönen. "L'utilizzo di agent indipendenti permette, per esempio, di fare **piazza pulita di molti falsi positivi**, riuscendo a individuare quali anomalie sono un possibile indizio di un attacco e quali invece sono provocate da semplici conflitti o errori a livello di networking o di applicazioni".

E le prospettive per il futuro? Mikko Hyppönen non esclude che, nel lungo periodo, un approccio di questo genere possa portare a un più profondo livello di condivisione delle informazioni tra i soggetti che si occupano di sicurezza informatica.

"Il problema principale è la compatibilità dei dati rilevati" puntualizza Hyppönen. "La collaborazione e la condivisione delle informazioni rappresenta però uno degli strumenti che gli esperti di sicurezza hanno a disposizione per contrastare in maniera sempre più efficace il cyber-crimine. L'idea che reti di AI distribuite comunichino tra loro anche oltre i confini del brand, quindi, è uno scenario plausibile".

Condividi l'articolo

Cina: addio a computer e software Made in USA in 3 anni

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/11/progetto-blackfin-f-secure-cambia-la-logica-dellintelligenza-artificiale/

Cina: addio a computer e software Made in USA in 3 anni

Dic 10, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Il governo di Pechino ha emesso una direttiva per fare piazza pulita dei prodotti tecnologici statunitensi. Sarebbero un rischio per la sicurezza.

La Cina "dichiara guerra" ai prodotti Made in USA e lo fa attraverso una direttiva che prevede per gli uffici pubblici e governativi l'abbandono di hardware e software prodotto negli Stati Uniti entro il 2022. Il provvedimento, che in realtà risale alla scorsa primavera, è stato reso pubblico dal **Financial Times**.

La direttiva, entro i confini cinesi, è conosciuta come 3-5-2, un nomignolo affibbiatole a causa della progressione prevista: riduzione del 30% dei dispositivi e software Made in USA nel 2020, del 50% nel 2021 e del rimanente 20% entro la fine del 2022.

La normativa non si applica per le aziende "private" con sede

in Cina e, fanno notare gli esperti, le sue tempistiche coincidono con l’iniziativa annunciata proprio a maggio e che prevede la creazione di un sistema operativo “fatto in casa” che andrebbe a sostituire **Windows**.

Ma quali sono le motivazioni di questa clamorosa iniziativa? Ufficialmente le motivazioni sono legate alla sicurezza. **Le autorità cinesi, infatti, considererebbero qualsiasi prodotto tecnologico (hardware o software) prodotto negli USA un potenziale rischio per la cyber-security**.

Non è escluso, però, che la logica sia anche dettata dagli sviluppi della guerra commerciale in corso tra le due super-potenze. L’amministrazione di **Donald Trump** ha infatti dimostrato in più occasioni di avere il “grilletto facile” per quanto riguarda i bandi commerciali.

E se i blocchi imposti alle aziende cinesi (prima tra tutte **Huawei**) hanno dimostrato di non avere una grande efficacia, un eventuale blocco commerciale che impedisse alle aziende statunitensi di vendere prodotti e servizi alla Repubblica Popolare Cinese potrebbe creare qualche problema, soprattutto nella pubblica amministrazione.

La mossa di Pechino, quindi, potrebbe essere un modo per acquisire una forma di indipendenza dagli USA e mettersi al riparo da eventuali problemi legati a una mossa del genere.

A fare le spese della nuova politica autarchica Made in China saranno principalmente aziende come **Dell**, **HP** e **Microsoft**. Ad avvantaggiarsene, probabilmente, **Lenovo**.

Condividi l’articolo

Progetto Blackfin: F-Secure cambia la logica dell’intelligenza artificiale La cassetta degli attrezzi del bravo hacker

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/10/cina-addio-a-computer-e-software-made-in-usa-in-3-anni/