Quando i rischi più gravi provengono dall’interno

Mag 28, 2020 Marco Schiaffino Approfondimenti, In evidenza, Scenario, Tecnologia 0

Le minacce non arrivano solo dall’esterno. Spesso gli incidenti informatici sono provocati da errori e da un’errata gestione a livello IT.

Gli esperti di cyber security, quando parlano di prevenzione, hanno la buona abitudine di guardare come prima cosa all’interno del perimetro. Il motivo? Nella maggior parte dei casi i veri rischi per la sicurezza si trovano proprio lì.

“Abbiamo l’abitudine a concentrarci in maniera ossessiva sui potenziali attacchi esterni” conferma **Massimo Carlotti di CyberArk**, società specializzata in *Privileged Access Management*. “La prima linea di difesa, però, deve essere schierata all’interno dei sistemi”.

D’altra parte l’esperienza (e la cronaca) dimostrano che una buona percentuale dei data breach non avvengono a causa di malware o di attacchi mirati da parte di hacker, ma da semplici errori o configurazioni errate che portano all’esposizione di dati sensibili.

Il caso ormai frequentissimo di implementazione di database e servizi privi di un’adeguata protezione è solo l’esempio più eclatante di un fenomeno che non accenna a diminuire.

Anche quando si parla di attacchi informatici a opera di cyber criminali, però, è evidente come una buona parte di questi sfrutti, in un modo o nell’altro, elementi di debolezza che provengono dall’interno.

“Sia quando si parla di incidenti provocati da errori umani, sia quando si tratta di attacchi informatici, il vero tema è quello della gestione dei privilegi” spiega Carlotti. “**In pratica il problema è sempre lo stesso: abbiamo delineato in maniera corretta il campo di azione concesso all’utente che ha provocato il danno o che ha subito l’attacco?**”

Quale che sia lo scenario, la logica è chiara: una limitazione dei privilegi, basata su rigorose policy, consente di ridurre il danno in maniera considerevole. Questo vale sia per l’errore umano, che verrà “contenuto” entro limiti che ne consentono la correzione, sia per gli attacchi veri e propri.

Spesso, infatti, gli attacchi dei pirati informatici prendono di mira utenti che, almeno teoricamente, non dovrebbero avere accesso a dati “interessanti”. In assenza di una segmentazione della rete e di una compartimentazione degli accessi basata sulle competenze, però, i cyber criminali trovano campo aperto anche quando sono riusciti a compromettere un bersaglio di basso profilo.

La soluzione, prosegue Carlotti, è quella di adottare la

filosofia **least privilege**, il principio per cui ogni utente dovrebbe avere accesso solo e soltanto alle risorse e agli strumenti di cui ha effettivamente bisogno. Un'impostazione che, secondo l'esperto di CyberArk, non viene sempre adottata.

"Il periodo che stiamo attraversando (legato all'emergenza **Covid-19** – ndr) vede per esempio un aumento esponenziale del lavoro da remoto" prosegue Carlotti. "Molte aziende hanno dovuto implementare servizi a distanza in tempi estremamente stretti, derogando alle policy di sicurezza che adottavano normalmente. Il risultato è un aumento incredibile della superficie d'attacco per i pirati e una maggiore incidenza di semplici errori".

L'implementazione di un sistema di controllo dei privilegi, oltre che dalla creazione di policy adeguate, passa necessariamente per una soluzione tecnica. La sfida, però, non è solo quella di "arginare" i possibili errori (e anche le attività dolose) ma di centrare il risultato senza introdurre ulteriori elementi di complessità.

L'introduzione di controlli e procedure di autenticazione,

infatti, rischiano di rendere le procedure complesse e il rischio, in questo caso, è che gli utenti finiscano per ignorarle o di cercare delle "scorciatoie" che finiscono inesorabilmente per compromettere gli stessi sistemi di protezione.

"Le tecnologie dovrebbero rendere le cose meno complesse" spiega Carlotti. "Quello che facciamo come CyberArk è di semplificare l'esperienza utente senza abbassare il livello di sicurezza. In caso contrario, qualsiasi precauzione rischia di rivelarsi inefficace".

Condividi l'articolo

Il malware Valak si evolve: ora punta alle grandi aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/28/quando-i-rischi-piu-gravi-provengono-dallinterno/?utm_source=rss&utm_medium=rss&utm_campaign=quando-i-rischi-piu-gravi-provengono-dallinterno

---

Il malware Valak si evolve: ora punta alle grandi aziende

Mag 28, 2020 Marco Schiaffino In evidenza, Malware, Minacce, News, RSS 0

Dopo mesi in cui lo hanno usato per diffondere altri malware, i suoi autori ne hanno modificato il codice per rubare informazioni sensibili.

Potremmo chiamarla “evoluzione della specie”, ma nel caso in questione è difficile classificarla come una buona notizia. A evolvere, infatti, è uno dei malware più complessi (e pericolosi) in circolazione: **Valak**.

Si tratta di una vecchia conoscenza per gli esperti di sicurezza: comparso alla fine del 2019, è stato utilizzato per mesi come dropper, cioè allo scopo di installare sui computer altri malware come **Ursnif** (ne abbiamo parlato ampiamente in questo articolo) e **IceID**.

I suoi autori, però, hanno deciso di andare oltre e sembrano aver lavorato sul codice del loro malware modificandolo con una certa frequenza. Secondo i ricercatori di **Cybereason Nocturnus**, negli ultimi sei mesi avrebbero sviluppato almeno 30 versioni differenti di Valak, trasformandolo in un malware “autonomo”.

Nel loro report, gli analisti spiegano che Valak ha una struttura modulare e adesso avrebbe la capacità di rubare informazioni sensibili dal computer infetto.

Gli attacchi individuati dagli esperti utilizzano come vettore un file di **Office** che sfrutta le funzionalità Macro per avviare l’esecuzione del codice di Valak. Una volta attivo, il

trojan installa una serie di payload aggiuntivi che forniscono, tra le altre cose, informazioni sulla macchina compromessa che vengono inviati ai server Command and Control.

I vari moduli, però, sembrano essere orientati specificatamente al mondo delle grandi aziende. Uno di questi (**Exchgrabber**) è pensato per prendere di mira Microsoft Exchange e infiltrare il sistema di posta aziendale, mentre **Netrecon** è finalizzato all'analisi della rete.

Non mancano funzioni tipiche dei trojan, come la possibilità di catturare screenshot della macchina infetta e un modulo che cerca di individuare quale tipo di software antivirus sia utilizzato.

Secondo gli autori del report, almeno per il momento, il trojan verrebbe utilizzato per colpire bersagli situati prevalentemente negli Stati Uniti e in Germania.

Condividi l'articolo

Quando i rischi più gravi provengono dall'interno Adesso eBay controlla la presenza di sistemi di controllo in remoto

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/28/il-malware-valak-si-evolve-ora-punta-alle-grandi-aziende/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-valak-si-evolve-ora-punta-alle-grandi-aziende

Adesso eBay controlla la presenza di sistemi di controllo in remoto

Mag 27, 2020 Marco Schiaffino In evidenza, News, Privacy, RSS, Scenario 0

Il sito di e-commerce ha introdotto un sistema di monitoraggio che esegue una scansione delle porte per individuare eventuali PC infetti.

Troppe truffe informatiche ed **eBay** corre ai ripari. La piattaforma di aste online si trova infatti coinvolta suo malgrado in molte attività dei cyber criminali, che sfruttano il sito per acquistare beni utilizzando gli account delle loro vittime.

La reazione degli sviluppatori di eBay, però, è piuttosto curiosa e ha sollevato molta curiosità tra gli esperti del

settore. **Avrebbero infatti introdotto un sistema che esegue una scansione di alcune porte del PC che si collega al sito**.

Ad accorgersene è stato uno sviluppatore che ha segnalato la cosa sul suo blog. Una piccola indagine da parte dei colleghi di **Bleeping Computer** ha confermato la presenza di un JavaScript chiamato **check.js** che avvia un collegamento a una serie di specifiche porte al momento del collegamento al sito.

Analizzando le porte sottoposte a scansione, i giornalisti hanno potuto associarle a numerosi strumenti di controllo o assistenza in remoto. **La loro opinione (che condividiamo) è che gli sviluppatori di eBay abbiano introdotto questo controllo per poter individuare eventuali PC controllati da pirati informatici**.

Fonte: Bleeping Computer

L’utilizzo di strumenti legittimi per il controllo remoto (come Remote Desktop) è ormai una prassi abituale per molti cyber criminali, che utilizzano i software come trojan o, in altri casi, usano le stesse porte utilizzate dai **VNC (Virtual Network Computing)** con i loro malware.

Il fatto che eBay sia particolarmente coinvolto in questo tipo di attività illecite è dovuto alle abitudini degli utenti, che spesso mantengono attivo il login al sito per poterlo visitare con facilità e maggiore frequenza, per esempio quando vogliono verificare l’andamento di un’asta.

Un comportamento che consente ai pirati informatici di accedere facilmente all’account e portare a termine gli acquisti fraudolenti.

Il JavaScript inserito nel sito eBay, che in un primo momento ha provocato qualche protesta tra gli esperti che hanno visto questa scansione come un’attività potenzialmente “intrusiva”, sarebbe quindi una forma di controllo che avrebbe lo scopo di mitigare il rischio di frodi ai danni dei suoi utenti.

Condividi l’articolo

Bug nel 70% delle applicazioni a causa delle librerie open source

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/27/adesso-ebay-controlla-la-presenza-di-sistemi-di-controllo-in-remoto/?utm_source=rss&utm_medium=rss&utm_campaign=adesso-ebay-controlla-la-presenza-di-sistemi-di-controllo-in-remoto

Bug nel 70% delle applicazioni a causa delle librerie open source

Mag 26, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

L'uso intensivo di librerie "aperte" e il riutilizzo del codice contribuisce a diffondere le falle di sicurezza in migliaia di applicazioni.

L'adozione della filosofia open source nella programmazione offre innumerevoli vantaggi, ma anche qualche problema. Uno di più importanti riguarda la sicurezza.

A confermarlo è una ricerca condotta da **Veracode**, che si concentra sull'utilizzo delle librerie open source nella creazione di applicazioni mobile e desktop. Il risultato dello studio è sconfortante: il 70% dei software si "porta dietro" bug e vulnerabilità.

Il report, che prende in esame più di **85.000 applicazioni e 351.000 librerie**, evidenzia un fenomeno che i programmatori conoscono benissimo: l'uso intensivo di librerie open source per la creazione del codice delle applicazioni.

Qual è il problema? Principalmente il fatto che una simile ragnatela di relazioni tra i vari software rende pressoché impossibile verificare se i componenti utilizzati siano afflitti da vulnerabilità. **A ogni passaggio della filiera, infatti, il livello di controllo si assottiglia fino ad**

arrivare a una situazione in cui le procedure di patching diventano pressoché impossibili.

Secondo gli autori del report, un semplice JavaScript può arrivare a utilizzare centinaia di librerie esterne, che vengono semplicemente integrate senza troppi controlli. A rendere le cose ancora più complicate, c'è il fatto che spesso sono disponibili varie versioni e che gli autori non sempre utilizzano una sintassi univoca per indicare il livello di aggiornamento.

D'altra parte, gli stessi ricercatori fanno notare come l'utilizzo di librerie per le funzioni base delle applicazioni sia uno dei tasselli fondamentali per consentire la creazione di funzionalità avanzate e rappresenti ormai un modo di lavorare che non ha alternative.

Da un punto di vista statistico, gli analisti di Veracode segnalano che l'utilizzo delle librerie varia a seconda del linguaggio utilizzato e, allo stesso modo, varia la quantità di bug presenti al loro interno.

I linguaggi in cui c'è una presenza maggiore di bug sono **Swift**; **PHP**; **.NET** e **Go**. Dal punto di vista della tipologia di vulnerabilità, la più diffusa sarebbe la classica **XXS** (Cross Site Scripting) seguita da bug nel sistema di accesso.

Il dato più preoccupante, però, è che per il 20% circa delle vulnerabilità sono disponibili dei Proof of Concept (PoC) che consentono di sfruttare un exploit. In altre parole: i pirati informatici non devono nemmeno fare la fatica di sviluppare una tecnica di attacco. Possono "pescarla" tra quelle disponibili.

Secondo i ricercatori, infine, quella delle librerie open source rappresenterebbe una vera "zona d'ombra" per quanto riguarda la ricerca delle vulnerabilità.

La buona notizia è che i bug in questione non sarebbero così "profondi" da richiedere interventi particolarmente impegnativi. Insomma: secondo gli autori sarebbe sufficiente una normale attività di verifica e una maggiore attenzione nella scelta dei componenti di codice in fase di sviluppo. Più facile a dirsi che a farsi.

Condividi l'articolo

Nuovo jailbreak per iOS. E funziona anche sulla nuova versione 13.5

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/26/bug-nel-70-delle-applicazioni-a-causa-delle-librerie-open-source/?utm_source=rss&utm_medium=rss&utm_campaign=bug-nel-70-delle-applicazioni-a-causa-delle-librerie-open-source

---

Nuovo jailbreak per iOS. E funziona anche sulla nuova versione 13.5

Mag 25, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Si chiama unc0ver 5.0 e .0 sfrutta una vulnerabilità zero-day del sistema Apple. Secondo gli autori "mantiene intatte le funzioni di sicurezza".

Non sono delle settimane particolarmente felici per **Apple**, per lo meno a livello di notizie per quanto riguarda la sicurezza dei suoi sistemi mobile. Dopo le illazioni provenienti da **Zerodium**, che ha parlato di un "eccesso di offerta" di exploit per iOS, ora spunta un nuovo **jailbreak**.

La nuova tecnica per scardinare il sistema di controllo Apple che impedisce di installare applicazioni esterne all'App Store è stata sviluppata da un team di sviluppatori capitanati (almeno a livello di comunicazione) da un programmatore che si firma **pwn20wnd**.

Il risultato è **unc0ver 5.0.0**, un software che consentirebbe di modificare il sistema operativo e installare applicazioni di terze parti non certificate da Apple su tutte le versioni di iOS successive alla 11.0, con qualche eccezione. La tecnica non funzionerebbe per le versioni comprese tra la 12.3 e la 12.3.2, così come tra la 12.4.2 e la 12.4.5.

Sul sito dedicato alla distribuzione del jailbreak, il team tiene a specificare che la nuova tecnica modifica ma non elimina il sistema di sandbox alla base dei sistemi di sicurezza di IOS. Insomma: secondo gli sviluppatori di

unc0ver, anche una volta effettuato il jailbreak non si dovrebbero temere attacchi hacker.

Una valutazione per lo meno discutibile che, pur avendo qualche fondamento (se il jailbreak smantellasse il sistema di compartimentazione dei dati sarebbe un vero disastro) non tiene conto che l'aggiramento dei controlli da parte di Apple mina alle fondamenta la stessa idea di "sicurezza" come interpretata dagli sviluppatori di Cupertino.

Visto e considerato che su iOS (proprio a causa del rigido sistema di sandbox) non è possibile utilizzare un antivirus, consentire l'installazione di qualsiasi applicazione è una strategia al limite del suicidio.

Tutta la vicenda, però, apre qualche legittima domanda sul livello di sicurezza complessivo di iOS. L'impressione, alimentata anche dalle già citate recenti dichiarazioni della dirigenza di Zerodium, è che sul sistema operativo dell'iPhone si siano concentrate tante (troppe) attenzioni da parte di ricercatori e hacker.

La comparsa di un jailbreak basato su una vulnerabilità zero-

day di iOS, insomma, potrebbe essere la conferma del fatto che negli ultimi tempi sono emerse davvero numerose vulnerabilità del sistema operativo e che nel prossimo futuro Apple si trovi a dover fronteggiare una vera emergenza.

Condividi l’articolo

RagnarLocker: il ransomware usa VirtualBox per sfuggire all’antivirus

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/25/sbuca-un-nuovo-jailbreak-per-ios-e-funziona-anche-sulla-nuova-versione-13-5/?utm_source=rss&utm_medium=rss&utm_campaign=sbuca-un-nuovo-jailbreak-per-ios-e-funziona-anche-sulla-nuova-versione-13-5

RagnarLocker: il ransomware usa VirtualBox per sfuggire all’antivirus

Mag 22, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

La curiosa tecnica messa a punto dai pirati informatici sfrutta VirtualBox per rendere più difficile la rilevazione dell'attività di codifica dei file.

Quando si pensa che non ci sia più nulla di nuovo da inventare, arriva un pirata informatico che è in grado di sorprendere con una nuova trovata.

Questa volta il tentativo di cambiare le carte in tavola nella gara a guardie e ladri tra cyber criminali ed esperti di sicurezza arriva dagli autori di un ransomware, che hanno avuto l'idea di utilizzare la virtualizzazione per offuscare l'attività del loro malware.

Il protagonista della vicenda è **RagnarLocker**, un crypto-ransomware che è stato individuato e analizzato dai ricercatori di **Sophos** (l'analisi è disponibile in questa pagina Internet) proprio ieri.

Il trucco adottato dai pirati, che secondo i ricercatori operano prendendo di mira principalmente le aziende e adattando i loro strumenti di attacco per ogni vittima, coinvolge un software di virtualizzazione piuttosto celebre.

Al posto di iniettare il loro ransomware nelle macchine compromesse, gli autori di RagnarLocker usano invece **Oracle VirtualBox**, un software per la virtualizzazione, che installano sul PC infettato.

Una volta avviato l’ambiente di virtualizzazione, i pirati eseguono una macchina virtuale che utilizza una versione “light” di Windows XP (MicroXP v0.82) che impostano in modo che abbia accesso a tutte le unità di memoria locali e condivise.

Il loro ransomware viene poi avviato all’interno della macchina virtuale, in modo che la sua attività abbia maggiori probabilità di passare inosservata ai sistemi di controllo degli antivirus.

La trovata è semplice ma geniale. Dal momento che l’attività dei ransomware è piuttosto difficile da individuare (la crittazione dei dati non è normalmente considerata un’attività “malevola”) molti antivirus fanno affidamento esclusivamente sul riconoscimento del codice malevolo.

Certo, il trucchetto non funziona con i sistemi di controllo più evoluti che contengono moduli specifici per individuare i ransomware. Il tentativo, in ogni caso, può essere considerato apprezzabile.

Condividi l’articolo

Allarme di Microsoft: “proteggete i server DNS da NXNSAttack

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/22/ragnarlocker-il-ransomware-usa-una-macchina-virtuale-per-sfuggire-allantivirus/?utm_source=rss&utm_medium=rss&utm_campaign=ragnarlocker-il-ransomware-usa-una-macchina-virtuale-per-sfuggire-allantivirus

Allarme di Microsoft: “proteggete i server DNS da NXNSAttack

Mag 21, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La nuova tecnica di DDoS consente ai pirati informatici di amplificare il traffico usato per l’attacco sfruttando un trucco particolarmente insidioso.

Non solo botnet IoT: il fenomeno degli attacchi DDoS (Distributed Denial Of Service) continua a essere estremamente variegato e i cyber criminali specializzati in questo tipo di “servizio” trovano costantemente nuovi stratagemmi per rendere più efficaci i loro attacchi.

È il caso di **NXNSAttack**, una tecnica di attacco descritta in un report a opera di alcuni ricercatori dell’**Università di Tel Aviv**, che adotta un sistema di amplificazione del traffico in grado di aumentarne esponenzialmente la potenza.

Come spiegano i ricercatori, l’unico prerequisito per portare un attacco del genere è quello di avere il controllo di un server DNS autoritativo (i server che gestiscono il **Domain Name System** di uno specifico dominio) e utilizzarlo come “sponda” per colpire altri Server DNS.

In pratica, la tecnica sfrutta lo stesso principio su cui è basato l’intero sistema DNS. La rete di server che gestisce il Domain Name System, infatti, è basata sulla collaborazione:

quando un server non è in grado di risolvere l’indirizzo richiesto, si rivolge a un altro. Più specificatamente, al server autoritativo del dominio di cui fa parte l’indirizzo richiesto.

Il sistema, però, permette anche di delegare il compito a un altro server autoritativo. Ed è qui che i ricercatori hanno trovato la possibilità di alimentare un attacco DDoS devastante.

Lo schema pubblicato sul blog **CZ.NIC** spiega il funzionamento di NXNSAttack in maniera estremamente intuitiva.

In pratica, l’attaccante invia una richiesta al resolver che fa riferimento a un dominio di cui ha il controllo e di cui gestisce il server DNS. Quando arriva la richiesta, il server delega dei falsi server DNS il cui indirizzo è compreso nel dominio della vittima.

Il resolver, a questo punto, cercherà di collegarsi ai falsi server richiedendo la risoluzione dell’indirizzo al server autoritativo della vittima, che in breve tempo verrà sommerso di richieste che non è in grado di risolvere. **Il livello di amplificazione, infatti, consentirebbe di moltiplicare per 1.620 volte il numero di pacchetti**.

Purtroppo, spiegano i ricercatori, non è possibile introdurre correzioni che escludano questo tipo di attacco, ma è possibile solo introdurre elementi di mitigazione.

È ciò che consiglia **Microsoft**, che sottolineando come non si siano ancora registrati attacchi che utilizzano questa tecnica, ha comunque “incoraggiato” gli amministratori IT ad adottare tutte le precauzioni utili a mitigare eventuali attacchi DDoS basati su NXNSAttack.

Condividi l’articolo

Attacchi di phishing con un trojan “legale”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/21/allarme-di-microsoft-proteggete-i-server-dns-da-nxnsattack/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-di-microsoft-proteggete-i-server-dns-da-nxnsattack

Attacchi di phishing con un trojan “legale”

Mag 20, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, Phishing, RSS 0

La campagna di phishing sfrutta l’emergenza Covid-19 per distribuire NetSupport Manager, un software di controllo remoto.

Come prendere il controllo di un computer riducendo al minimo le probabilità che l’antivirus invii un allarme quando viene scaricato il trojan? Semplice: basta utilizzare un software di controllo remoto “legale”.

L’allarme relativo a questa strategia è stato lanciato da **Microsoft**, che in un tweet ha segnalato una campagna di diffusione che sfrutta **NetSupport Manager**, un tool di controllo remoto che viene normalmente utilizzato nelle aziende per gestire l’amministrazione a distanza di computer e dispositivi.

> *We’re tracking a massive campaign that delivers the legitimate remote access tool NetSupport Manager using emails with attachments containing malicious Excel 4.0 macros. The COVID-19 themed campaign started on May 12 and has so far used several hundreds of unique attachments. pic.twitter.com/kwxOA0pfXH*
>
> *— Microsoft Security Intelligence (@MsftSecIntel) May 18, 2020*

Il vettore di attacco utilizzato dai pirati informatici non è particolarmente originale: si tratta di file **Excel** che utilizzano i comandi **Macro** per avviare il download e l'installazione del software. Naturalmente l'utente deve assecondare l'attività dei comandi abilitando la funzionalità Macro.

Poco originale anche l'esca utilizzata: i fogli di calcolo contengono infatti informazioni sulla diffusione del Covid-19 all'interno degli Stati Uniti che sembrano provenire dall'ormai celebre **Johns Hopkins Center**. Una tecnica, quella che sfrutta la pandemia, che sembra però mantenere una buona efficacia anche settimane dopo l'avvio dell'emergenza.

Una volta installato, NetSupport Manager consente ai pirati informatici di controllare in remoto il computer eseguendo qualsiasi tipo di comando a distanza. Agli occhi di un qualsiasi utente, può sembrare un'applicazione legittima che solleva ben pochi sospetti. Tanto più che il nome "Netsupport Client Application" può facilmente passare per un'applicazione di sistema.

Secondo i ricercatori, i cyber criminali utilizzano lo strumento di controllo remoto per installare sul computer compromesso altri programmi e script per “massimizzare” l’impatto.

Condividi l’articolo

Cyber guerriglia incrociata tra Israele e Iran

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/20/attacchi-di-phishing-con-un-trojan-legale/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-di-phishing-con-un-trojan-legale

Cyber guerriglia incrociata tra Israele e Iran

Mag 19, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 0

I servizi segreti di Tel Aviv hanno messo K.O. i sistemi di un porto commerciale iraniano come rappresaglia a un precedente cyber-attacco di Teheran.

I fatti risalgono al 9 maggio, ma la conferma ufficiale della responsabilità del **governo di Tel Aviv**, spiegano in un articolo i giornalisti del **Washington Post**, è arrivata solo in questi giorni.

In quel sabato il porto iraniano di **Shahid Rajaee**, importante centro di smistamento commerciale affacciato sul Golfo Persico, ha vissuto ore di vero caos provocate da un collasso di tutti i sistemi informatici che gestiscono il traffico navale e la logistica per il carico e lo scarico delle merci.

L’attacco, secondo fonti iraniane, avrebbe colpito solo “alcuni operatori privati” collegati alla gestione del porto. Stando ai rilevamenti effettuati (tra cui foto satellitari) le conseguenze sarebbero state però piuttosto “importanti”, con code e blocchi a livello logistico.

L’attacco sarebbe una rappresaglia portata dal governo israeliano nei confronti di Teheran in seguito a un’altra azione di cyber-guerriglia che avrebbe preso di mira, il giorno precedente, alcune reti per la distribuzione dell’acqua sul territorio di Israele.

Le fonti citate dal Washington Post sottolineano che l’attacco dell’8 maggio avrebbe preso di mira non solo i sistemi di distribuzione dell’acqua, ma anche quelli che gestiscono l’immissione di cloro e altre sostanze chimiche nel sistema idrico.

Insomma, dopo il clamoroso precedente di Stuxnet, il malware utilizzato da USA e Israele per sabotare le centrali di

arricchimento dell’uranio iraniane, il Medioriente sembra confermare il suo ruolo di “terreno di sperimentazione” per gli attacchi informatici che prendono di mira i sistemi industriali.

Condividi l’articolo

Storie di ransomware: 5000 IT Manager raccontano com’è andata

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/19/cyber-guerriglia-incrociata-tra-israele-e-iran/?utm_source=rss&utm_medium=rss&utm_campaign=cyber-guerriglia-incrociata-tra-israele-e-iran

---

CyberArk: prima di tutto proteggere gli account privilegiati

Mag 18, 2020 Marco Schiaffino Approfondimenti, Gestione dati, In evidenza, Scenario, Tecnologia 0

Nell’ecosistema IT gli utenti non sono tutti uguali. Ecco perché è indispensabile riuscire a valutare i livelli di privilegi e predisporre le difese.

Se la protezione dell’identità digitale è un dei fulcri della sicurezza informatica. La sua declinazione pratica non può essere gestita in maniera acritica, come se tutti gli account presenti in azienda fossero equivalenti. Per implementare un sistema di protezione a prova di bomba è necessario infatti stabilire delle priorità a cui attenersi.

“Troppo spesso si è portati a identificare gli account privilegiati esclusivamente con quelli che hanno poteri di amministrazione” spiega **Massimo Carlotti di CyberArk**, società specializzata in *Privileged Access Management*. “In realtà una valutazione di questo tipo deve tenere conto di molti più aspetti”.

Per esempio dal contesto. Con la progressiva introduzione di servizi cloud, per esempio, il livello di agibilità dei singoli account ha spesso valore diverso all’interno o all’esterno del perimetro fisico del network. “Nel momento in cui un account ha poteri di gestione di determinati servizi a livello cloud, dovrebbe essere considerato alla stregua di un vero e proprio amministratore, anche se in una visione tradizionale a livello IT non ne avrebbe le caratteristiche” specifica Carlotti.

Secondo l’esperto di CyberArk, la determinazione del livello di privilegio di un account non può essere fatta in maniera statica, ma richiede una valutazione dinamica che consideri tutte le possibili ripercussioni “a valle” dell’uso delle credenziali, attraverso una valutazione dinamica del rischio.

Quello che bisogna chiedersi, in buona sostanza, è che cosa può essere effettivamente fatto utilizzando quelle credenziali e quale sia il rischio per l’integrità dei sistemi e dei dati aziendali.

“CyberArk adotta un approccio basato sull’idea di un blueprint, che offre linea guida molto articolate e aiuta a definire un approccio basato sulla valutazione del rischio” precisa Massimo Carlotti.

Un approccio particolarmente utile per evitare di lasciare scoperte delle “aree grigie”, come accade troppo spesso, per esempio, in ambito **Saas (Software as a Service)** quando le aziende non realizzano che la definizione dei privilegi rappresenta il pilastro fondamentale nella gestione della sicurezza degli applicativi.

Tanto più che, nella pratica, si tende a dimenticare che un singolo account non è necessariamente collegato a una sola persona fisica. È il caso delle situazioni in cui sono previste interazioni tra applicazioni, che comunicano tra di loro utilizzando credenziali.

“Nella maggior parte dei casi, i privilegi di accesso **application to application** vengono impostate in fase di implementazione e poi non vengono più modificate” spiega Carlotti. “Questo però non significa che non ci siano individui che sono in possesso di quelle credenziali”.

Gli accessi gestiti in questo modo hanno anche un altro problema: il loro utilizzo non viene registrato dalla maggior parte dei sistemi **SIEM (Security Information and Event Management)** tra i log significativi per l'analisi degli eventi di sicurezza. Il motivo è semplice: comprenderle nell'analisi creerebbe un "rumore di fondo" eccessivo, che finirebbe per saturare i sistemi di controllo.

Una situazione che apre la strada a possibili abusi e incidenti informatici, per esempio nel caso in cui le credenziali in questione finiscono nelle mani di un pirata informatico in seguito alla violazione di un endpoint con cui erano condivise.

"La soluzione di CyberArk tiene conto di tutti questi elementi e utilizza un sistema di mediazione che consente, per esempio, di eseguire una rotazione delle credenziali ogni volta che vengono utilizzate" spiega Carlotti. **Il vantaggio è duplice: oltre a ridurre l'esposizione delle credenziali, si può fare in modo che queste vengano cambiate frequentemente, riducendo esponenzialmente il rischio di una violazione**.

L'analisi del rischio, inoltre, viene effettuata dinamicamente, attraverso una serie di regole che permettono

di individuare tempestivamente eventuali anomalie nell’utilizzo delle credenziali e bloccare immediatamente qualsiasi abuso.

Condividi l’articolo

QNodeService: il trojan (quasi) invisibile agli antivirus

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/18/cyberark-prima-di-tutto-proteggere-gli-account-privilegiati/?utm_source=rss&utm_medium=rss&utm_campaign=cyberark-prima-di-tutto-proteggere-gli-account-privilegiati