Cybersecurity e IoT, l’Enisa pubblica le nuove linee guida per la supply chain. Il report

L’Enisa, l’agenzia dell’Unione Europea per la sicurezza informatica, ha pubblicato le nuove linee guida sulla protezione dell’intera catena di approvvigionamento dell’IoT, inclusi hardware, software e servizi.

Il rapport ***“Guidelines for Securing the IoT – Secure Supply Chain for IoT”***, pubblicato ieri dall’agenzia si basa sulla pubblicazione del ciclo di sviluppo del software sicuro dello scorso anno concentrandosi sui processi effettivi della catena di approvvigionamento utilizzata per sviluppare prodotti IoT, integrando al contempo il precedente studio di Enisa sulle raccomandazioni di sicurezza di base per l’Internet of Things.

IoT e minacce informatiche

In una dichiarazione, l’agenzia ha affermato che le catene di approvvigionamento stanno attualmente affrontando una vasta gamma di minacce, dalle minacce fisiche alle minacce alla sicurezza informatica, mentre le organizzazioni hanno meno visibilità e comprensione di come la tecnologia acquisita viene sviluppata, integrata e implementata rispetto al passato.

L’indagine identifica l’esistenza di componenti e fornitori di terze parti non attendibili e la gestione delle vulnerabilità di componenti di terze parti come le due principali minacce

alla catena di fornitura dell’Internet of Things.

La pubblicazione analizza le diverse fasi del processo di sviluppo, esplora le considerazioni più importanti sulla sicurezza, identifica le buone pratiche di cui tenere conto in ogni fase e offre ai lettori risorse aggiuntive da altre iniziative, standard e linee guida.

Per approfondire

Per saperne di più: IoT

> *Cybersecurity e IoT, l’Enisa pubblica le nuove linee guida per la supply chain. Il report*

Agent Tesla, una nuova campagna malspam interessa l’Italia

Una nuova campagna malspam italiana che, sfruttando alcune caselle di posta elettronica compromesse, veicola il RAT Agent Tesla inviando allegati con estensione .xlsm è stata individuata dal **CSIRT** questa settimana.

Il Remote Access Trojan Agent Tesla

Agent Tesla nato come semplice keylogger e infostealer, nel tempo ha assunto i connotati di un potente RAT per il

controllo completo da remoto del target, aggiungendo ulteriori capacità spyware in grado di carpire oltre che impostazioni e account wifi anche credenziali di client di posta elettronica, VPN e browser, enumerando file di log, di registro e di configurazione e instaurando dei canali di comunicazione con centraline di comando per mezzo di protocolli standard e legittimi quali HTTP, SMTP e FTP.

Attraverso il phishing e cambiando opportunamente il tema delle campagne malspam e le tecniche di evasione, i criminal hacker sono riusciti a diffondere nel corso del tempo diverse varianti del codice Agent Tesla. Per esempio alcune di esse, al fine di eludere i sistemi di sicurezza con metodi di anti-rilevamento, non sono state iniettate direttamente nell'allegato e-mail (che in tal caso avvia solo la catena infettiva) ma fatte scaricare in stadi successivi attraverso binari eseguibili o addirittura inoculate in applicativi vulnerabili già presenti sulle macchine target.

L'ultima campagna malspam Italiana

La recente analisi condotta dal CSIRT parla di una campagna malspam che invia e-mail da caselle di posta compromesse a enti pubblici e società private italiani, in cui il messaggio, riportante loghi e nominativi reali, invita il destinatario ad aprire come allegato un file .xlsm ovvero un foglio di calcolo excel abilitato per le macro ("Ordine numero 045202020********.xlsm", MD5: 1c6acfad45e467f2f2ca0807856c9102) facente riferimento ad un ipotetico ordine effettuato presso un'azienda tecnica specializzata. In realtà la macro excel, una volta abilitata dall'utente, avvia la catena d'infezione malevola con un processo deputato a reperire alcune informazioni di sistema e quindi a avviare, in seconda istanza, uno script PowerShell per scaricare un binario eseguibile (btl.exe, MD5: a216c284ec62f79239204d358030b247) dall'indirizzo http://95.214.8[.]54.

Le passate campagne malevoli rilevate

Questa è solo l'ultima di una serie di campagne veicolanti il malware Agent Tesla e che hanno interessato società e utenze italiane negli ultimi mesi. Di seguito un elenco di alcuni alert segnalati dal CSIRT anche con ulteriori e puntuali aggiornamenti per evento.

- **Ottobre 2020.** Il malware è veicolato tramite messaggio e-mail contenente un falso ordine di acquisto merce, il cui mittente si finge una società italiana. Il falso allegato di acquisto è in realtà un file .DAT che contiene un file eseguibile malevolo.
- **Settembre 2020.** Il malware è veicolato tramite messaggio e-mail contenente in allegato un archivio in formato GZ. L'oggetto del messaggio di posta, contenente un finto codice identificativo fa riferimento a una presunta comunicazione da parte della compagnia di trasporti internazionali DHL. L'allegato è un file eseguibile che avvia il processo d'infezione e di comunicazione con il server C2 finalizzato al download del relativo payload.
- **Agosto 2020**. Il malware è veicolato tramite messaggi e-mail inviati impersonando diverse società italiane. L'oggetto della mail fa riferimento a un'offerta di quotazione per un ordine di acquisto e il falso allegato altro non è che un file immagine .ISO che custodisce al suo interno il file eseguibile (.exe) malevolo.
- **Giugno 2020**. Il malware è veicolato tramite messaggio e-mail avente come oggetto una presunta copia di pagamento con relativa data di spedizione. Il testo, scritto in italiano, invita gli utenti ad aprire l'archivio allegato e compresso in formato .7z. Anche in questo caso il file eseguibile contenuto distribuisce il malware Agent Tesla.

Le azioni di difesa consigliate

Agent Tesla un RAT in continua evoluzione e periodicamente aggiornato dai suoi sviluppatori sempre con nuove funzionalità, attestandosi nel primo semestre 2020 in testa alle classifiche dei malware più diffusi, rappresenta, di fatto, una reale minaccia che propinata principalmente, come visto, attraverso una mescolanza di tecniche di social engineering e phishing deve essere a tutti i costi contrastata.

Risulta, pertanto, fondamentale adottare come misure di difesa non solo accorgimenti hardware/software ma anche azioni fondate sulla security awareness dell'elemento umano e atte a sensibilizzare l'utente a non ritenere, sbagliando, che una frode o una truffa non possa concretizzarsi anche per il tramite di strumenti spesso ritenuti puramente virtuali, privi di trabocchetti e scollegati dal mondo reale.

A tal proposito valgono le seguenti e utili raccomandazioni aziendali:

- limitare le funzionalità delle macro presenti nei documenti Office che attivano automaticamente connessioni a Internet;
- fornire periodiche sessioni di formazione finalizzate a riconoscere il phishing anche per il tramite di servizi di simulazioni di attacchi;
- tenere sempre aggiornati apparati e strumenti di sicurezza con le patch disponibili, valutando anche l'eventuale implementazione degli indici di compromissione periodicamente indicati dal CSIRT.

https://www.key4biz.it/agent-tesla-una-nuova-campagna-malspam-interessa-litalia/329773/

Bonus Bici, attenzione al sito truffa con la a accentata

Il Bonus Bici è partito oggi con numerose polemiche (oltre 400mila persone in coda), sito in tilt e non funzionante.

Ma un'altra problematica si è insediata all'interno del click day: i siti fake creati apposta dai cybercriminali per sfruttare il traffico intenso per rubare i dati degli utenti o compiere truffe informatiche.

Bonus Bici: tra disservizi e siti fake

Segnaliamo infatti il sito truffa **buonomobilità.it** (con la a accentata), un dominio registrato su **CloudFlare** pur non essendo il sito internet ufficiale.

Il sito con l'accento è un falso e risulta essere molto pericoloso in quanto è stato indicizzato molto bene, perché risultava nei primi posti su Google subito sotto a quello ministeriale.

Il sito corretto a cui accedere è buonomobilita.it.

Bonus mobilità

Il buono mobilità è un contributo pari al 60% della spesa

sostenuta – fino a un massimo di 500 euro – per l'acquisto di biciclette, anche a pedalata assistita, veicoli per la mobilità personale a propulsione prevalentemente elettrica (monopattini, hoverboard e segway).

Da oggi è possibile chiedere il bonus attraverso il sito. Sarà un clic-day a causa dei pochi fondi stanziati e "buoni erogati secondo l'ordine temporale di arrivo delle richieste".

https://www.key4biz.it/bonus-bici-attenzione-al-sito-truffa-con-la-a-accentata/328995/

Attacco hacker alla campagna elettorale di Donald Trump. Rubati 2,3 milioni di dollari in Wisconsin

Un gruppo di hacker ha sottratto al Partito repubblicano nel Wisconsin 2,3 milioni di dollari da un conto corrente dedicato a finanziare attività per la rielezione del presidente Donald Trump.

Lo ha riferito ieri il leader locale dei Repubblicani, **Andrew Hitt,** all'Associated Press.

Il Partito aveva notato attività sospette il 22 ottobre scorso e aveva contattato immediatamente il **Federal Bureau of Investigation (Fbi**), che – spiega Hitt – sta attualmente indagando sull'episodio.

Come è successo

Secondo il presidente del Partito repubblicano nel Wisconsin, gli hacker sarebbero riusciti a manipolare le fatture di quattro fornitori ingaggiati per inviare materiale postale e gadget elettorali per la rielezione di Trump. Così, quando il Partito ha provveduto al saldo dovuto, il denaro è andato agli hacker invece che ai fornitori.

Il Wisconsin è uno degli Stati in bilico che potrebbero avere un ruolo decisivo per l'esito delle elezioni del prossimo 3 novembre. Qui nel 2016 ha vinto Trump con un distacco di meno di 23 mila voti, ma quest'anno i sondaggi danno in netto vantaggio il candidato democratico **Joe Biden**, che sarà proprio nel Wisconsin venerdì prossimo.

Donald Trump e i problemi con la cybersecurity

Il partito repubblicano nelle ultime settimane è letteralmente bersagliato da criminali informatici. L'ultima attacco era stato inflitto martedì al sito della campagna elettorale di Trump *donaldjtrump.com* dove un gruppo di criminal hacker sconosciuti era riuscito a sabotare il sito del Tyconn mandando in onda il seguente messaggio: " *Questo sito è sequestrato. Il mondo ne ha abbastanza delle fake news diffuse quotidianamente dal presidente.*

È ora si conosca la verità", continuava il messaggio aggiungendo che il gruppo di hacker fosse in possesso di informazioni compromettenti sul presidente e la sua famiglia, sia sul coronavirus che sulle prossime elezioni. *"Il trump-gov è coinvolto nell'origine del coronavirus e sta collaborando con gli stranieri per manipolare le elezioni".*

L'attacco informatico, a detta di **Tim Murtaugh**, responsabile della campagna di Trump, non ha avuto conseguenze dal punto di

vista di data breach.

https://www.key4biz.it/attacco-hacker-alla-campagna-elettorale-di-donald-trump-rubati-23-milioni-di-dollari-in-wisconsin/328537/

La condivisione delle informazioni al centro della cyber resilienza, l'Europa punta sui centri Isac

La legislazione europea in tema di sicurezza informatica, come il Cybersecurity Act e la Direttiva NIS, promuove in tutti i Paesi dell'Unione la creazione dei centri di condivisione e analisi di informazioni inerenti alla cyber sicurezza nazionale.

Si tratta degli *Information sharing and analysis centres* o **Isac**, partenariati pubblico-privati per il potenziamento della difesa informatica di organizzazioni operative nel settore dei servizi essenziali.

Gli Isac raccolgono, esaminano e diffondono informazioni relative alle minacce informatiche da condividere tra tutti i membri aderenti, fornendo loro conoscenze, strumentazioni e *best practice* di riferimento per mitigare e contrastare i cyber attacchi.

Le guide Enisa per i centri Isac europei

L'Agenzia europea per la cyber sicurezza (**Enisa**) ha il compito di sostenere, promuovere e aiutare la creazione dei centri Isac in tutti gli Stati europei, facendo leva su una migliore cooperazione tra forze intergovernative e nazionali impegnate nel contrasto al cyber crime ad ogni livello.

Fiducia, collaborazione e condivisione delle informazioni sono i tre pilastri alla base del meccanismo Isac. L'Enisa si impegna, in questa fase di lancio, ad offrire a chiunque ne faccia richiesta delle **guide pratiche e delle "*cassette per gli attrezzi*" (*toolkit*)** utili alla nascita degli Isac o al rinnovo di quelli già preesistenti.

Il lavoro si svolgerà in quattro step principali e provvede a fornire alle organizzazioni tutti i documenti e gli strumenti necessari a far nascere un centro Isca. Una prima fase è quella in cui si stabiliscono gli obiettivi generali (***build phase***) e i meccanismi di cooperazione; una seconda più esecutiva (***run phase***); una terza fase di valutazione (***evalutation phase***) per monitorare l'andamento dei progetti e misurarne i risultati provvisori; un'ultima dedicata allo sviluppo finale delle attività (***develop phase***) e al loro impatto generale.

Proiezioni 2021 e mercato globale cyber sicurezza

Secondo nuove proiezioni elaborate da Forrester, almeno il 35% di tutti i data breach attesi per il 2021 sarà dovuto ad incidenti informatici interni alle organizzazioni (oggi il dato è al 25%).

Probabilmente si tratta del risultato diretto dello **smart**

working, del lavorare da casa da parte di una fetta crescente di dipendenti, che potrebbe aumentare del **+300% entro un anno**, ma anche della facilità con cui si spostano continuamente dati e dell'utilizzo costante di device personali anche in ambito lavorativo.

In un contesto del genere, secondo un Rapporto pubblicato da Research and Markets, gli investimenti in tecnologie, piattaforme e servizi di cyber security aumenteranno progressivamente, con un tasso di crescita medio annuo del +8% tra il 2020 ed il 2025 (Cagr).

Tra cinque anni, secondo tali stime, **il mercato globale della cyber security potrebbe raggiungere i 174 miliardi di dollari** di valore.

> *La condivisione delle informazioni al centro della cyber resilienza, l'Europa punta sui centri Isac*

Cybercrime, la botnet KashmirBlack prende di mira le piattaforme CMS. Come difendersi

Un team di ricercatori statunitense ha fornito dei report dettagliati riguardo a una nuova botnet denominata **KashmirBlack** che, sulla base dei numerosi indizi trovati, si

ritiene sia opera di *“Exect1337”* un membro del gruppo hacker indonesiano **PhantomGhost**.

Tale botnet utilizzata molto probabilmente per attività di cripto mining, spam e *defacement* per diffondere ed espandere il proprio raggio di azione (arruolando nuovi bot) si propaga attraverso exploit di note piattaforme CMS (**WordPress, Joomla!, PrestaShop, Magento, Drupal, Vbulletin, OsCommerence, OpenCart e Yeager**) utilizzando, inoltre, i servizi basati su cloud **Github, Pastebin e Dropbox** come mezzo per celare e gestire la botnet stessa.

KashmirBlack: modalità di funzionamento

I ricercatori hanno individuato, durante la propria attività di telemetria (avvenuta tra novembre 2019 e fine maggio 2020, seppur la bonet risulti tutt’oggi ancora operativa) circa 700.000 tentativi di attacchi giornalieri con ben 285 bot in azione, ma il numero potrebbe molto probabilmente essere ancor più consistente anche in considerazione dell’evoluzione osservata.

La botnet KashimirBlack inizialmente di medio volume con capacità standard si è presto trasformata in una ben progettata e complessa infrastruttura, ad oggi, costituita da un server C2 con più di 60 server surrogati come parte integrante del proprio impianto.

Il server di comando e controllo (C2) capace di gestire centinaia di bot svolge principalmente tre compiti:

1. fornisce uno script Perl per l’infezione del server vittima;
2. riceve dai bot i rapporti sui risultati;
3. fornisce ai bot le istruzioni di attacco.

I bot, invece, possono trovarsi secondo necessità in due stati

differenti:

- Attivo. I “spreading bot” possono effettuare operazioni tese ad estendere la dimensione della botnet, comunicando con il server C2 per ricevere indicazioni sui nuovi target, eseguire attacchi brute force e installare backdoor come teste di ponte;
- Standby. I “pending bot” restano in attesa di cambiare stato, ascoltando periodicamente il canale di comunicazione instaurato con il server C2.

Vulnerabilità sfruttate per la diffusione

Secondo quanto riportato dallo studio, l’attività monitorata starebbe ancora generando diversi attacchi contro migliaia di vittime sparse in tutte il mondo, diffondendosi grazie alla compromissione di siti web in esecuzione su piattaforme CMS non aggiornate e potenzialmente vulnerabili anche a certi exploit su plugin, librerie e componenti interne:

- PHPUnit Remote Code Execution – CVE-2017-9841
- jQuery file upload vulnerability – CVE-2018-9206
- ELFinder Command Injection – CVE-2019-9194
- Joomla! remote file upload vulnerability
- Magento Local File Inclusion – CVE-2015-2067
- Magento Webforms Upload Vulnerability
- CMS Plupload Arbitrary File Upload
- Yeager CMS vulnerability – CVE-2015-7571
- WordPress TimThumb RFI Vulnerability – CVE-2011-4106
- Uploadify RCE vulnerability
- vBulletin Widget RCE – CVE-2019-16759
- WordPress install.php RCE
- WordPress xmlrpc.php Login Brute-Force attack
- WordPress multiple Plugins RCE
- WordPress multiple Themes RCE
- Webdav file upload vulnerability

KashmirBlack: come difendersi

Per impedire e rilevare possibili tentativi di attacco i ricercatori hanno fornito diversi consigli e dettagli tecnici specifici.

In particolare, ciò che raccomandano agli amministratori dei siti web è di assicurare innanzitutto:

- l'aggiornamento periodico e la corretta configurazione non solo dei CMS ma anche degli eventuali moduli extra di terze parti;
- un'adeguata gestione delle password per contrastare gli attacchi brute force;
- una protezione ulteriore dei propri siti, tramite l'adozione di firewall WAF utili per le applicazioni Web;
- un controllo preventivo rimuovendo processi sospetti, plugin e temi inutilizzati oltre che negare l'accesso a file e directory fondamentali di sistema e configurazione PHP.

Cybercrime, la botnet KashmirBlack prende di mira le piattaforme CMS. Come difendersi

---

Ransomware e Covid, l'FBI avverte gli ospedali: 'Alto rischio di attacchi, si

rischia il blocco delle strutture’. Il report

I criminal hacker stanno prendendo di mira il settore sanitario utilizzando virus malevoli e attacchi *ransomware*, c’è il rischio di una *“minaccia informatica imminente”*.

L’annuncio arriva direttamente dall’FBI e altre due agenzie governative nel report “***Ransomware Activity Targeting the Healthcare and Public Health Sector***” disponibile qui.

Gli enti di sicurezza degli Stati Uniti affermano infatti di avere *“informazioni credibili”* e lanciano l’allarme per ospedali e operatori sanitari già alle prese con una pandemia che finora ha fatto più di 227mila vittime nel Paese.

La minaccia arriva mentre gli ospedali statunitensi sono alle prese con un numero crescente di casi di coronavirus. Per questo motivo le agenzie federali hanno esortato gli operatori sanitari statunitensi a prendere *“precauzioni tempestive e ragionevoli”* per proteggere le loro reti.

Le agenzie consigliano inoltre di cambiare regolarmente le password e di utilizzare l’autenticazione a più fattori.

Hanno incoraggiato gli operatori sanitari a proteggere i loro sistemi operativi e i software il prima possibile e a condurre regolarmente scansioni antivirus e antimalware.

L’FBI al personale sanitario: difendetevi dai Ransomware

Il ransomware è un tipo di software dannoso utilizzato dai criminali informatici per crittografare i file degli utenti

fino al pagamento di un riscatto. Le istituzioni sanitarie sono state vittime frequenti di ransomware per diversi anni negli Stati Uniti e nel mondo.

Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

- sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);
- contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli

Il mese scorso, un sospetto attacco ransomware ha interrotto l'assistenza ai pazienti in un'ampia catena di ospedali e cliniche che operano negli Stati Uniti e in Gran Bretagna. In Germania, un attacco ransomware alla struttura informatica di un pronto soccorso, che ha portato all'interruzione dei sistemi e alla sospensione delle attività ambulatoriali e di emergenza, ha portato al decesso di una donna che non ha potuto ricevere le cure sanitarie urgenti di cui necessitava, ritardate a causa del trasferimento in altra struttura.

Per approfondire

Scarica il report in esclusiva ***Ransomware Activity Targeting the Healthcare and Public Health Sector*** qui

https://www.key4biz.it/ransomware-e-covid-lfbi-avverte-gli-ospedali-alto-rischio-di-attacchi-si-rischia-il-blocco-delle-strutture-il-report/328250/

La Cybersecurity ha a disposizione le tecnologie adeguate? Scarica il Report

Un’organizzazione indipendente che riunisce esperti del settore per discutere su come migliorare la cybersecurity, **Debate Security**, ha pubblicato una ricerca sulle prestazioni inefficaci del mercato della sicurezza informatica.

Sulla base di oltre 100 interviste con leader aziendali e grandi imprese, insieme a fornitori, organizzazioni di valutazione, agenzie governative, associazioni di settore e regolatori, la ricerca di Debate Security fa luce sul perché i fornitori di tecnologia non sono incentivati a fornire prodotti più efficaci a ridurre il rischio cibernetico.

L’inefficacia della cybersecurity? Questioni economiche e non tecnologiche

Il report Cybersecurity Technology Efficacy: Is Cybersecurity The New “Market for Lemons” ?, sostiene l’opinione che i problemi di efficacia nel mercato della cybersecurity siano

principalmente dovuti a questioni economiche, non tecnologiche. La ricerca affronta tre temi chiave e alla fine arriva a un consenso su come affrontare un nuovo modello:

- **La tecnologia non è così efficace come dovrebbe essere**

Il 90% dei partecipanti ha riferito che la tecnologia di sicurezza informatica non è efficace come dovrebbe essere quando si tratta di proteggere le organizzazioni dal rischio informatico.

- **Il problema di fondo è l'economia, non la tecnologia**

Per la ricerca il 92% dei partecipanti ha riferito che c'è una rottura nel rapporto di mercato tra acquirenti e fornitori, con molti che vedono asimmetrie informative profonde. Al di fuori del Governo, oggi pochi acquirenti utilizzano una valutazione dell'efficacia della sicurezza informatica dettagliata e indipendente come parte del loro processo di approvvigionamento di sicurezza informatica e nemmeno le organizzazioni più grandi hanno dichiarato di avere le risorse per condurre da sole tutte le valutazioni. Di conseguenza, i fornitori sono incentivati □□a concentrarsi su altre caratteristiche del prodotto e sul marketing, riducendo le priorità dell'efficacia della tecnologia di sicurezza informatica, uno dei numerosi segni classici di un "mercato dei limoni".

- **A meno che gli acquirenti non richiedano una maggiore efficacia, la regolamentazione potrebbe essere l'unico modo per affrontare il problema.**

Il 70% degli intervistati ritiene che una valutazione indipendente e trasparente della tecnologia aiuterebbe a risolvere il crollo del mercato. Stabilire standard sulla valutazione della tecnologia piuttosto che sulla tecnologia stessa potrebbe impedire il soffocamento dell'innovazione.

Scarica il report

Clicca qui per scaricare il report

https://www.key4biz.it/la-cybersecurity-ha-a-disposizione-le-tecnologie-adeguate-scarica-il-report/327972/

Cyber attacco russo alle reti governative USA, FBI: “Elezioni a rischio”

E’ da febbraio di quest’anno, che la rete di uffici, agenzie e amministrazioni locali del Governo degli Stati Uniti è sotto attacco informatico.

È quanto affermato in un **documento** congiunto pubblicato ieri dall’**Fbi** (Federal bureau of investigation) e dalla Cybersecurity and infrastructure security agency (**Cisa**).

Obiettivo degli attacchi copiare dati sensibili e relativi alla sicurezza nazionale, tra cui file governativi, configurazioni delle reti, password di accesso, contenuti delle email, dati identificativi del personale, credenziali di qualsiasi tipo.

Non solo, perchè gli investigatori hanno trovato traccia di esfiltrazione di codici per reimpostare le password, istruzioni reti IT, elenco fornitori, informazioni sulle centrali degli acquisti, le stampe dei badge di accesso alle

strutture e molto altro.

Secondo l’Fbi e l’Agenzia per la cyber sicurezza americana si è trattato di una serie di attacchi portati a termine dal gruppo hacker russo noto con il nome di **Energetic Bear**, ma già identificato con altri nomi come TEMP.Isotope, Bersek Bear, Dragonfly, Havex, Koala.

L’azione del gruppo ha coinvolto dozzine di reti governative federali e statali, sfruttando **vulnerabilità note**, a partire da quelle delle reti private virtuali (Vpn) e dai bug di Windows.

Gli hacker potrebbero aver agito per conto di Mosca e per un motivo evidente: destabilizzare la politica nazionale americana, anche in vista delle imminenti **elezioni presidenziali di novembre**, ma anche per minare la **sicurezza nazionale** (l’esfiltrazione di dati ha riguardato anche aziende nell’elenco dei fornitori dell’aereonautica militare americana).

Già a settembre, Microsoft aveva dichiarato pubblicamente che l’unità dell’intelligence militare russa (Gru), responsabile delle interferenze del 2016, con molta probabilità era tornata all’attacco mettendo nel mirino collaboratori, consulenti e think tank associati sia ai deputati e senatori dem che repubblicani.

> *Cyber attacco russo alle reti governative USA, FBI: “Elezioni a rischio”*

Luxottica, pubblicati sul dark web i dati rubati dal recente attacco hacker

Per molti, la reazione di **Luxottica** all'attacco hacker subito di recente, era stata da manuale. Ma secondo **Odisseus**, esperto indipendente di sicurezza informatica, non sembra affatto così.

Attraverso un tweet, Odisseus fa sapere che il gruppo criminale **Nefilim** ha pubblicato sul **dark web 2 GB** di dati che sembrano provenire dall'hacking dello scorso 20 settembre ai danni della multinazionale.

> *The #Nefilim hacker group published #Luxottica's files after the #ransomware attack.*
>
> *Two file lists and 2 GB of data stored in the #darkweb:*
>
> *– LUXOTICA_Human_Res_part1_filelist_part1.txt*
> *– LUXOTICA_Finance_part1_filelist.txt*
> *pic.twitter.com/i16PHl9Tbh*
>
> *– Odisseus (@_odisseus) October 20, 2020*

Nel tweet di **Odisseus** ci sono due screenshot relativi a due file. Uno fa riferimento alle risorse umane, l'altro al dipartimento finanziario.

Non sappiamo nel dettaglio il contenuto dei due file, ma c'è il concreto rischio che siano incluse informazioni personali sui dipendenti e dati sensibili di carattere finanziario.

Attacco ransomware a Luxottica, i dettagli

Su key4biz siamo stati tra i primi a riportare la notizia dell'attacco informatico alla società guidata da **Leonardo Del Vecchio**. L'hack, che ha riguardato in particolare le sedi Luxottica di Agordo e Sedico, in provincia di Belluno, ha provocato il blocco della produzione e la sospensione dei turni degli operai.

Se in un primo momento si è parlato di gravi problemi informatici, come rete fuori uso, il blocco dei computer e l'impossibilità ad eseguire qualsiasi operazione, sarebbe poi stato confermato un attacco ransomware. Per la società è stato

un tentativo di violare i sistemi informatici che non avrebbe avuto esito positivo grazie all’attivazione dei meccanismi di difesa.

Il rischio di una multa

Secondo quanto riportato dal sito *Bleeping Computer* i criminali informatici avrebbero sfruttato una vulnerabilità nota dall’inizio dell’anno nei prodotti VPN di Citrix for Cyber-Attacks, con la quale ottenere credenziali per l’accesso e la diffusione all’interno di una rete. La stessa vulnerabilità che avrebbe consentito l’attacco ransomware ad un ospedale tedesco pochi giorni prima, dalle conseguenze ben peggiori.

Se il data breach però dovesse risultare vero, diventerebbe un grave danno all’immagine della multinazionale. Inoltre l’azienda potrà ricevere una sanzione per violazione della privacy in materia di GDPR da parte dell’Autorità Garante.

https://www.key4biz.it/luxottica-pubblicati-sul-dark-web-i-dati-rubati-dal-recente-attacco-hacker/327173/