Cashback di Stato, nuova truffa malware per gli utenti italiani. L’allarme del CERT-AgID

È in corso in Italia una campagna malspam volta a veicolare un malware facendo leva sul recente programma di rimborso in denaro per acquisti effettuati con strumenti di pagamento elettronici: il **Cashback di Stato**.

Lo ha rilevato il **CERT-AgID,** che, grazie ai suoi esperti, ha permesso di rilevate che il link nel testo non scarica un file pdf come riportato.

Fonte: Cert-Agid

Cashback di Stato: attenzione all’email truffa

Il file scaricato non è un documento pdf come riportato nel link, spiega il CERT-AgID, ma si tratta di un file eseguibile scritto in Visual Basic 6 con doppia estensione.

Il malware è scritto in VB6 ed utilizza un server FTP su Altervista per lo scambio di informazioni con l’autore.

All’avvio il malware si occupa di gestire la propria persistenza copiandosi nella home dell’utente ed usando il registro di sistema, dopodichè colleziona le informazioni

sulla macchina della vittima e le salva sul server FTP.

Infine scarica un modulo aggiuntivo (keylogger) dal server FTP e avvia un timer che recupera i comandi da eseguire sempre da un file presente sul server FTP.

Come difendersi

Gli utenti e le organizzazioni possono far fronte a questa tipologia di attacchi verificando scrupolosamente le email ricevute e attivando le seguenti misure aggiuntive:

- diffidare dalle comunicazioni non attese che invitano ad aprire allegati in riferimento a transazioni economiche, fatture o verifiche di pagamento;
- considerare la disattivazione delle macro o qualora non fosse possibile impedire che le stesse siano in grado di instaurare connessioni verso risorse esterne non note;
- implementare filtri nel gateway di posta elettronica per bloccare, se non necessario, gli allegati di posta elettronica costituiti da allegati associati a estensioni non comuni (.iso) o generalmente associate a malware (.dll, e .exe).

Cashback di Stato, nuova truffa malware per gli utenti italiani. L'allarme del CERT-AgID

Allerta Polizia Postale: Emotet prende di mira le

istituzioni scolastiche

Il framework Emotet

Il trojan bancario Emotet, apparso in natura per la prima volta nel 2014, si è nel tempo evoluto fino a diventare un vero e proprio framework criminale multi forma, rappresentando di sicuro una delle principali minacce nel 2018, nel 2019 e nei primi mesi del 2020 in pieno inizio era COVID-19.

Come segnalato da vari report di sicurezza, le botnet Emotet hanno iniziato a veicolare malspam, utilizzando consuete e ben collaudate tecniche con campioni e-mail, spesso recapitati come risposte in contesti di comunicazioni preesistenti, contenenti allegati o link URL afferenti il più delle volte a file Microsoft Office malevoli, con lo scopo ultimo di propagare anche altre forme di software malevolo come trojan (Trickbot) e ransomware (Ryuk) sui computer delle malcapitate vittime.

Infatti spesso i criminal hacher sfruttano indirizzi e-mail conosciuti alle stesse vittime non solo per sferrare attacchi di spear phishing, aggiungendo credibilità allo spam, ma anche per distribuire malware. Nella fattispecie, è noto come l'e-mail intercettate e carpite da Emotet vengano trasmesse a server presidiati e utilizzate per future campagne fraudolente.

La campagna in atto che interessa le istituzioni scolastiche

Questa volta l'allarme a lanciarlo è proprio la Polizia

Postale con un comunicato semplice e diretto https://www.commissariatodips.it/notizie/articolo/false-mail-contenenti-malware-e-allapparenza-provenienti-da-istruzioneit/index.html :

“È in corso una massiccia campagna di diffusione del malware “EMOTET” attraverso mail che sembrerebbero provenire da caselle riconducibili al dominio @istruzione.it, con un allegato in formato Zip protetto da password (presente nel testo della mail), da scaricare.

Il trojan ha diverse finalità tra cui in via prioritaria l’accesso a contatti ed informazioni personali anche di tipo bancario…”

Inoltre in un tweet delle scorse ore gli specialisti di sicurezza TGSOFT hanno reso noto https://twitter.com/VirITeXplorer/status/1346062116994887685?s=19 sulla base della loro continua attività di monitoraggio che numerosi sono gli indirizzi coinvolti e che risultano appartenenti a domini istituzionali del MIUR: istruzione.it, pec.istruzione.it, posta.istruzione.it, postarcert.istruzione.it.

In particolare nel periodo compreso tra il 28 e 31 dicembre 2020, **il team segnala una consistente catalogazione di indirizzi e-mail coinvolti e relativi al dominio “istruzione.it” con 2858 indirizzi utilizzati come falsi mittenti (ovvero account di posta** elettronica compromessi da EMOTET**), 452 indirizzi utilizzati come mittenti reali (ovvero** account di posta elettronica che sono stati compromessi non necessariamente da EMOTET) **e ben 7177 indirizzi di posta elettronica destinatari di m**alspam proveniente dalla botnet in oggetto, e relativi al dominio “pec.istruzione.it” con numeri che sarebbero più contenuti anche se sempre rilevanti: 598 indirizzi relativi a falsi mittenti, 339 indirizzi relativi a mittenti reali e 2274 destinatari.

Come proteggersi

Poiché, come già accennato, uno dei moduli Emotet consente di rubare anche credenziali e quindi di diffondersi mediante messaggi infetti provenienti da utenti presenti tra i nostri contatti, per evitare di contribuire inconsapevolmente alla catena di propagazione, è importante proteggere gli account, oltreché utilizzando password robuste e diverse per ogni profilo, attivando se possibile meccanismi di autenticazione multi fattore e servizi di alerting e procedendo, quanto prima, a verificare se il proprio indirizzo di posta elettronica sia stato in qualche modo compromesso, consultando il database **HAVEiBeenEMOTET** https://www.haveibeenemotet.com/index.php progressivamente tenuto aggiornato dagli analisti di TGSOFT con gli indirizzi e-mail utilizzati nella campagne di diffusione Emotet.

In ogni caso risultano anche utili allo scopo le raccomandazioni di protezione che solitamente si suggeriscono per contrastare generalmente il phishing, quali ad esempio prestare la massima attenzione quando si ricevono e-mail di provenienza sospetta o da mittenti sconosciuti e evitare di aprire allegati o abilitare l'esecuzione di macro Microsoft Office, anche se le azioni potrebbero sembrare apparentemente legittime.

https://www.key4biz.it/allerta-polizia-postale-emotet-prende-di-mira-le-istituzioni-scolastiche/337855/

Deepfake, tra furto

d’identità e minacce per le aziende. Come difendersi

L’utilizzo di app basate su algoritmi di AI per la manipolazione di immagini, video e audio noti come “Deepfake” è in continuo aumento. Eppure, non sempre le aziende che sviluppano queste app tengono conto dei rischi a cui potrebbero essere esposti gli utenti.

I **deepfake** sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

Allarme per le aziende

Nel 2021 vedremo l’emergere di deepfake negli attacchi alle imprese, non per seminare necessariamente confusione o caos di massa, ma più per amplificare gli attacchi di ingegneria sociale.

Video e registrazioni di dirigenti sono spesso già disponibili per attività di marketing, social media e altro ancora. Gli attaccanti potrebbero inserire deepfake in tentativi di phishing (che si allontaneranno dalla posta elettronica per sfruttare altre piattaforme come le applicazioni di chat e collaborazione) per rendere le comunicazioni manipolate ancora più autentiche. Soprattutto al giorno d’oggi, dove sempre più organizzazioni si affidano al video come mezzo di comunicazione tra dirigenti e dipendenti, gli aggressori possono approfittare di questo livello di fiducia instillato.

Sono comuni, ad esempio, le e-mail di phishing che chiedono le password – ma cosa succederebbe se a quell'e-mail seguisse un messaggio urgente del CEO su WhatsApp? Gli attaccanti potrebbero anche utilizzare video manipolati di dirigenti sui social per invogliare clienti, dipendenti, partner e altro ancora a cliccare su link dannosi – creando nuove vie di attacco più ampie per gli attori dannosi.

Come proteggersi dai deepfake

Le grandi imprese del digitale (piattaforme social media, motori di ricerca, ecc.) stanno già studiando e applicando delle **metodologie per il contrasto al fenomeno**, come algoritmi di intelligenza artificiale capaci di individuare i deepfake o sistemi per le segnalazioni da parte degli utenti, e stanno formando team specializzati nel monitoraggio e contrasto al deepfake. E le **Autorità di protezione dei dati personali** possono intervenire per prevenire e sanzionare le violazioni della normativa in materia di protezione dati.

Tuttavia, il primo e più efficace strumento di difesa è rappresentato sempre dalla responsabilità e dall'attenzione degli utenti. Ecco allora alcuni suggerimenti del Garante Privacy per gli utenti:

- Evitare di diffondere in modo incontrollato immagini personali o dei propri cari. In particolare, se si postano immagini sui social media, è bene ricordare che le stesse potrebbero rimanere online per sempre o che, anche nel caso in cui si decida poi di cancellarle, qualcuno potrebbe già essersene appropriato.
- Anche se non è semplice, si può imparare a riconoscere un deepfake. Ci sono elementi che aiutano: l'immagine può appare pixellata (cioè un pò "sgranata" o sfocata); gli occhi delle persone possono muoversi a volte in modo innaturale; la bocca può apparire deformata o troppo grande mentre la persona dice alcune cose; la luce e le

ombre sul viso possono apparire anormali.

- Se si ha il dubbio che un video o un audio siano un deepfake realizzato all'insaputa dell'interessato, occorre assolutamente evitare di condividerlo (per non moltiplicare il danno alle persone con la sua diffusione incontrollata). E si può magari decidere di segnalarlo come possibile falso alla piattaforma che lo ospita (ad esempio, un social media).
- Se si ritiene che il deepfake sia stato utilizzato in modo da compiere un reato o una violazione della privacy, ci si può rivolgere, a seconda dei casi, alle autorità di polizia (ad esempio, alla Polizia postale) o al Garante per la protezione dei dati personali.

Deepfake, tra furto d'identità e minacce per le aziende. Come difendersi

---

Ho.mobile, confermato il breach di alcuni dati di una parte dei clienti "Non dati bancari né di traffico"

L'operatore **ho.mobile** ha confermato il furto di dati di alcuni clienti. Lo ha fatto sapere oggi in un comunicato, spiegando che *"dopo le ulteriori verifiche effettuate, che sono tuttora*

in corso, è emerso che sono stati sottratti illegalmente ***alcuni dati di parte della base clienti*** *con riferimento solo ai dati anagrafici e tecnici della SIM*. Con questi dati, spiega la società, *"fare SIM Swapping non è possibile per chiunque entri in possesso della banca dati, dal momento che per effettuare il cambio di operatore ora serve una copia dei documenti dell'intestatario".*

L'azienda precisa che non sono stati in alcun modo sottratti dati relativi al traffico (sms, telefonate, attività web, etc.), né dati bancari o relativi a qualsiasi sistema di pagamento dei propri clienti. Inoltre

"*Ho. mobile,* si legge nel comunicato, *"comunica di aver già sporto denuncia alla Autorità inquirente e informato il Garante della Privacy, con i quali sta lavorando in stretto contatto".*

ho mobile: il furto di dati annunciato da Bank Security

Il presunto furto di dati era stato annunciato il 28 dicembre dall'account di sicurezza informatica **Bank Security**. Tra i dati sensibili trafugati secondo l'account di sicurezza ci sarebbero nomi, email, indirizzi di casa del lavoro, codici fiscali, partite iva, numeri di telefono, ma anche il codice ICCID, cioè quello che identifica la SIM e che ne permette la portabilità.

"*In queste ore stiamo procedendo ad informare solo i clienti ho. Mobile coinvolti, e abbiamo già attivato ulteriori e nuovi livelli di sicurezza per mettere la clientela al riparo da potenziali minacce. Ulteriori azioni a protezione dei dati sottratti sono in corso di implementazione e verranno comunicate ai clienti",* continua la nota di ho.mobile. *"Inoltre,* spiega l'operatore, *"stiamo assistendo a diversi fenomeni speculativi sui social network e pertanto invitiamo i*

clienti a verificare direttamente con i canali ufficiali di ho. Mobile ogni informazione ed eventuale esigenza di supporto”.

Possibilità di cambiare sim gratis per gli utenti

“Stiamo procedendo ad informare solo i clienti coinvolti nel data breach. Chi è cliente ho.mobile e non ha ricevuto nessuna comunicazione non è coinvolto nel data breach” fa sapere l’operatore. *“Abbiamo già attivato ulteriori e nuovi livelli di sicurezza per mettere la clientela al riparo da potenziali minacce. Ulteriori azioni a protezione dei dati sottratti sono in corso di implementazione e verranno comunicate ai clienti.“*

Per tutti i clienti ho.mobile l’azienda ha messo a disposizione la possibilità di procedere gratuitamente alla sostituzione della propria SIM presso i punti vendita autorizzati.

Non solo ho.mobile

Nel 2020 numerose aziende italiane sono rimaste vittime di attacchi informatici che si sono intensificati e accelerati durante la pandemia. **Luxottica**, la più grande produttrice mondiale di montature per occhiali da vista e da sole, lo scorso settembre è stata colpita da un’imponente attacco che ha causato la sospensione del secondo turno produttivo negli stabilimenti di **Agordo** e Sedico, nel bellunese, e il blocco delle attività produttive in Cina.

Anche il Gruppo **Carraro,** azienda italiana leader internazionale nel comparto delle macchine agricole, ha subito nel 2020 un grave attacco informatico. Un ransomware ha paralizzato i sistemi informatici che controllano praticamente tutta l’attività del gruppo, da quella amministrativa a quella produttiva, altamente automatizzata da robot.

A giugno invece la vittima è stata **Geox**, azienda trevigiana di calzature. dove anche lì un ransomware ha colpito i sistemi IT dell'azienda.

https://www.key4biz.it/ho-mobile-confermato-il-breach-di-alcuni-dati-di-una-parte-dei-clienti/337490/

Dark Web, in vendita i dati di oltre 200 milioni di cittadini cinesi

I dati privati di oltre 200 milioni di dati di cittadini cinesi sono in vendita sul dark web. La scoperta arriva dai ricercatori di cybersecurity di Cyble, che attraverso un lungo post sul loro blog, hanno comunicato la presenza di tre database in vendita in alcuni forum.

I database presenti nel darkweb

"Durante il nostro monitoraggio di routine sul Dark web", si legge nel comunicato del team di ricerca, *"abbiamo trovato diversi post in cui criminal hackers mettono in vendita i relativi database".*

Fonte: cybleinc.com
Secondo gli esperti le informazioni presenti sono legate ai cittadini cinesi della contea di **Gong’an** e alle piattaforme **Weibo** e a **QQ**. Le informazioni riguardano nomi, data di nascita, sesso, indirizzi e numeri di telefono.

Weibo è una piattaforma basata sulla promozione delle relazioni con gli utenti per condividere, diffondere e ricevere informazioni. Tramite il sito Web o l’app mobile, gli utenti possono caricare immagini e video. In questo caso uno dei criminal hacker ha messo in vendita un archivio con 41,8 milioni di dati.

Fonte: cybleinc.com
QQ è un servizio software di messaggistica istantanea e un portale web sviluppato dal gigante tecnologico cinese **Tencent**. QQ offre servizi come giochi online, musica, acquisti, microblogging, film e software di chat vocale e di gruppo. In questo caso, spiegano i ricercatori, il criminale informatico ha messo in vendita i dettagli di 192 milioni di utenti cinesi sul darkweb.

Fonte: cybleinc.com

Se le informazioni dovessero essere confermate, invece, sarebbe certo che si tratterebbe del più grande db di data leak mai messo in vendita dai criminal hacker.

https://www.key4biz.it/dark-web-in-vendita-i-dati-di-oltre-200-milioni-di-cittadini-cinesi/337418/

Ho.mobile, l’operatore: “Nessun furto di dati”. Occhio alle campagne malspam via email ed sms

La notizia che i dati dei clienti di **Ho.mobile** sarebbero in vendita sul dark web è stata smentita dall’operatore italiano.

La smentita di Ho.mobile

Ho.mobile, con un comunicato, ha smentito che ci sia stato un attacco, e un conseguente furto dei dati di Ho.mobile: *“Con riferimento ad alcune indiscrezioni pubblicate da organi di stampa*, scrive la compagnia nel comunicato, *ho.mobile non ha evidenze di accessi massivi ai propri sistemi informatici che abbiano messo a repentaglio i dati della customer base. Abbiamo avviato in collaborazione con le autorità investigative le indagini per ulteriori approfondimenti”.*

Il presunto furto di dati annunciato il 29 dicembre dall’account di sicurezza informatica **Bank Security** ha destato preoccupazione per gli utenti.

Tra i dati sensibili trafugati secondo Bank Security ci sarebbero nomi, email, indirizzi di casa del lavoro, codici fiscali, partite iva, numeri di telefono, ma anche il codice ICCID, cioè quello che identifica la SIM e che ne permette la portabilità.

Criminal hacker potrebbero sfruttare campagne malspam

I principali esperti di sicurezza informatica adesso temono che i criminal hacker possano sfruttare il momento per incrementare *le campagne malspam contro gli utenti.*

Si potrebbe infatti assistere all'invio di messaggi che con carattere di urgenza invitano le potenziali vittime a riempire form per la raccolta dei loro dati oppure aprire documenti contenenti malware infetti.

Come difendersi?

La prima e più importante forma di difesa è la prudenza.

Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.

Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze.

Ad esempio:

- non aprire mai allegati con estensioni "strane" (ad esempio, allegati con estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
- scaricare preferibilmente app e programmi da market ufficiali, i cui gestori effettuano controlli sui prodotti

- se si usa un pc, si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).

Ho.mobile, l'operatore: "Nessun furto di dati". Occhio alle campagne malspam via email ed sms

---

Phishing, +220% di attacchi nel 2020. Il report

Il report Report "Phishing and Fraud 2020"

Gli incidenti di phishing sono aumentati del 220% durante il culmine della pandemia globale, rispetto alla media annuale.

Sono questi i dati evidenziati nel nuovo Report "Phishing and Fraud 2020" degli F5 Labs. Nel 2020 il COVID-19 continua ad essere un fattore significativo nell'aumento dei tentativi di phishing e frode da parte dei criminali informatici.

Sulla base dei dati del Security Operations Center (SOC) degli esperti di sicurezza, il numero degli incidenti di phishing

nel 2020 sarebbe ogni anno destinato ad aumentare del 15%. Un risultato ampiamente superato e che potrebbe ulteriormente variare a seguito della seconda ondata della pandemia.

I tre tipi di attacchi principali

I tre obiettivi principali degli attacchi e di phishing tramite email che sfruttano COVID-19 come esca sono stati identificati in

- donazioni fraudolente a falsi enti di beneficenza
- raccolta illecita di credenziali
- diffusione di malware

L'opportunismo degli aggressori che sfruttano disagi e debolezze emotive causate dalla pandemia è stato ulteriormente dimostrato a seguito dell'analisi dei log di Certificate Transparency (certificati digitali emessi da un'autorità di certificazione ritenuta pubblicamente attendibile).

Il numero di certificati che utilizzano i termini "covid" e "corona" ha raggiunto la cifra record di 14.940 a marzo, con un aumento del 1102% rispetto al mese precedente.

Phishing: Amazon, Apple, PayPal, Netflix i domini più utilizzati

Come già evidenziato nelle edizioni del report degli anni precedenti, la creatività dei truffatori quando si tratta di scegliere nomi e indirizzi dei loro siti di phishing è sempre in crescita.

Da inizio 2020 ad oggi, il 52% dei siti destinati ad azioni di phishing ha utilizzato nomi e identità di brand scelti con cura per i propri indirizzi web. Utilizzando i dati di **Webroot**, gli analisti hanno scoperto che Amazon è stato il

brand più sfruttato nella seconda metà del 2020, con **Paypal, Apple, WhatsApp, Microsoft Office, Netflix e Instagram** che comparivano nella lista dei 10 marchi "impersonificati" più diffusi.

Tracciando il furto di credenziali, gli esperti hanno osservato come i criminali tentino di utilizzare le password rubate entro quattro ore dall'attacco di phishing. Alcuni attacchi si verificano addirittura in tempo reale, per finalizzare l'acquisizione di codici di sicurezza di autenticazione a più fattori (MFA). I criminali informatici sono diventati anche più efficienti nelle loro offerte per dirottare URL affidabili, spesso anche gratuitamente. Da soli, i siti WordPress rappresentano il 20% degli URL generici di phishing nel 2020. Nel 2017 la cifra era pari al 4,7%.

I siti fraudolenti utilizzano certificati HTTPS validi

Il 2020 ha visto anche i criminali intensificare i propri sforzi nel dissimulare i siti fraudolenti, facendoli apparire il più autentici e innocui possibile.

Le statistiche hanno rilevato che **la maggior parte dei siti di phishing sfrutta la crittografia**, in particolare il 72% utilizza certificati HTTPS validi per ingannare le vittime.

Quest'anno, il 100% delle drop zone – ovvero le destinazioni dei dati rubati dal malware – ha utilizzato la crittografia TLS (rispetto all'89% del 2019).

Per approfondire

Per scaricare il report "Phishing and Fraud 2020" clicca qui

https://www.key4biz.it/phishing-220-di-attacchi-nel-2020-il-report/336467/

Bitcoin e criptovalute, nel 2021 sempre più utilizzate per chiedere riscatti. Il trend

La recente risalita dei Bitcoin è una notizia che fa felici anche gli hacker. La regina delle criptovalute sarà tra le protagoniste nel traffico economico del cybercrimine nel 2021. Lo rende noto Kaspersky, individuando i principali trend che dovrà affrontare il panorama finanziario nel prossimo anno.

Criptovalute: bitcoin e monero al top nel 2021

Oltre i bitcoin, secondo i ricercatori di sicurezza, nel 2021 aumenteranno altri metodi di scambio di denaro digitale, con la crescita di quelli che promettono ancora maggior privacy. Le estorsioni ai danni degli utenti punteranno proprio a questo: ricatti e pagamenti ancora tramite Bitcoin ma con il consolidamento di piattaforme, come **Monero**, che consentono una maggiore tutela dell'anonimato, con conseguente difficoltà nel rintracciare il passaggio tra i portafogli.

Il furto stesso di **Bitcoin** diventerà ancora più presente quando molte nazioni rischieranno la povertà a causa della pandemia. Con il crollo delle economie e il calo delle valute locali, un numero maggiore di persone potrebbe interessarsi al mondo della criminalità informatica, con un conseguente

aumento dei casi. Grazie al successo delle loro operazioni, i responsabili degli attacchi ransomware alzeranno le somme di denaro richieste alle vittime, con la promessa di non pubblicare le informazioni rubate.

Bitrail: identificato in Italia il responsabile della 'buco' di 120 milioni di euro

Lo scorso 21 dicembre la Polizia Postale ha identificato l'autore del "più grande attacco cyberfinanziario in Italia, uno dei più grandi mai realizzati nel mondo nel settore delle criptovalute": si tratta di un fiorentino di 34 anni responsabile di un "buco" pari a 120 milioni di euro sulla piattaforma informatica hackerata Bitgrail. Oltre 230 mila risparmiatori truffati.

L'uomo è accusato di frode informatica, auto-riciclaggio e bancarotta fraudolenta. La polizia postale italiana ha posto così *"una pietra miliare a livello mondiale nel settore delle indagini sulle criptovalute, con un'indagine unica nel suo genere ad alto impatto tecnologico".*

"Per la prima volta in Italia e in Europa – ha sottolineato la polizia postale – *si sono documentate condotte fraudolente e distrattive in danno di investitori, poste in essere integralmente su piattaforme informatiche e l'impiego di monete virtuali".*

https://www.key4biz.it/bitcoin-e-criptovalute-nel-2021-sempre-piu-utilizzate-per-chiedere-riscatti-il-trend/336760/

Cybercrime, deepfake e fattore umano le principali minacce per le aziende

Il 2021 sarà per la sicurezza informatica un anno pieno di insidie. La pandemia ha determinato una drastica accelerazione delle iniziative digitali in tutti i settori di mercato in quanto le aziende hanno dovuto adottare rapidamente tecnologie a supporto della produttività e della continuità del business.

Sia che si trattasse di portare nuovi strumenti di collaborazione o di spostare infrastrutture e applicazioni critiche nel cloud, tutto è diventato più distribuito, aumentando notevolmente, di conseguenza, le opportunità per i potenziali aggressori.

Che impatto avrà la convergenza di queste forze ed eventi sulla sicurezza informatica nei prossimi 12 mesi? Eccone due particolarmente importanti: deepfake e dipendenti.

I deepfake diventano una minaccia anche per le aziende

Qualcosa può essere troppo enfatizzato e rappresentare comunque una minaccia emergente? Questo è il caso dei deepfake – un termine che è simulatamene abusato e un esempio di come gli attaccanti continueranno a personalizzare i loro attacchi.

In sintesi, i deepfake sono video o immagini, sintetici o manipolati, in cui una persona viene sostituita con la somiglianza di qualcun altro. Da un punto di vista culturale,

il concetto di deepfake ha dominato i notiziari come una potenziale minaccia che potrebbe influenzare l'opinione pubblica, danneggiare la reputazione e altro ancora. Spesso questi attacchi fanno notizia, ma finiscono per essere relativamente poco efficaci.

Tuttavia, man mano che la tendenza della catena di attacchi personalizzati continua, vedremo l'emergere di deepfake negli attacchi alle imprese – non per seminare necessariamente confusione o caos di massa, ma più per amplificare gli attacchi di ingegneria sociale.

Video e registrazioni di dirigenti sono spesso già disponibili per attività di marketing, social media e altro ancora. Gli attaccanti potrebbero inserire deepfake in tentativi di phishing (che si allontaneranno dalla posta elettronica per sfruttare altre piattaforme come le applicazioni di chat e collaborazione) per rendere le comunicazioni manipolate ancora più autentiche. Soprattutto al giorno d'oggi, dove sempre più organizzazioni si affidano al video come mezzo di comunicazione tra dirigenti e dipendenti, gli aggressori possono approfittare di questo livello di fiducia instillato.

Sono comuni, ad esempio, le e-mail di phishing che chiedono le password – ma cosa succederebbe se a quell'e-mail seguisse un messaggio urgente del CEO su WhatsApp? Gli attaccanti potrebbero anche utilizzare video manipolati di dirigenti sui social per invogliare clienti, dipendenti, partner e altro ancora a cliccare su link dannosi – creando nuove vie di attacco più ampie per gli attori dannosi.

I dipendenti

La pandemia ha creato un'enorme tensione sui dipendenti e sulle loro famiglie. L'incertezza economica e il passaggio al lavoro e alla scuola a distanza ha messo molti in un territorio inesplorato. Queste nuove sfide potrebbero probabilmente spingere un numero maggiore di dipendenti a

prendere decisioni sbagliate quando si tratta di sicurezza informatica e creare una nuova ondata di insider malintenzionati.

Come abbiamo già osservato nel 2020, gli attaccanti offrono sempre più spesso ai dipendenti con accesso privilegiato incentivi finanziari allettanti per condividere o "accidentalmente" far trapelare le proprie credenziali. Inoltre, l'accesso privilegiato sul dark web è più popolare che mai, e alcune ricerche indicano che gli aggressori sono disposti a pagare per ottenere l'accesso privilegiato alle reti aziendali, alle VPN e alle workstation.

La potenziale ricompensa finanziaria, combinata con l'aumento dell'ansia economica, porterà alla nascita di nuove minacce che le organizzazioni faticheranno a fronteggiare.

https://www.key4biz.it/cybercrime-deepfake-e-fattore-umano-le-principali-minacce-per-le-aziende/336238/

Cybersecurity, i principali trend per il 2021

Con la diffusione della pandemia di Coronavirus si è visto un incremento dell'attività dei criminali informatici in tutto il mondo. In modo particolare FBI, Europol e società di intelligence hanno visto un particolare aumento della diffusione di attacchi ransomware, programmi malevoli che possono *"infettare"* un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni

dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".

Ma cosa succederà l'anno prossimo e come sarà necessario modificare le strategie aziendali man mano che il panorama delle minacce continuerà a evolvere? I ricercatori di sicurezza di **Proofpoint**, cercano di rispondere analizzando i principali trend previsti per il 2021.

Ransomware

Il ransomware rimane la principale fonte di preoccupazione per i CISO. Come consolidata macchina da soldi per i cybercriminali, era solo una questione di tempo prima che i suoi principali creatori arrivassero a sviluppare nuovi metodi di estorsione, in particolare con la minaccia di diffondere le informazioni rubate. Nel 2021, in seguito alla rapida accelerazione dell'adozione del cloud guidata dalla pandemia COVID-19, ci aspettiamo che anche gli attacchi ransomware si evolvano verso il cloud. Molte aziende ora ospitano porzioni importanti dei loro dati sensibili in repository esterni basati nel cloud, e questi archivi sono spesso meno visibili a chi si occupa di sicurezza – spesso anche non così protetti o sottoposti a backup in modo da essere a prova di cifratura criminale. Nel 2021, i professionisti della sicurezza possono aspettarsi di vedere un numero sempre maggiore di ransomware indirizzati verso lo storage cloud per massimizzare l'impatto e aumentare la leva per incrementare i profitti.

Malware

La stragrande maggioranza dei cyberattacchi inizia via e-mail e praticamente il 100% del malware si basa su un'azione dell'utente per la compromissione iniziale. I cybercriminali hanno ormai ben chiaro che cercare di sfondare in altri modi (ad esempio usando gateway VPN senza patch) è possibile, ma molto più difficile grazie al grande lavoro che i

professionisti della sicurezza hanno svolto nel corso degli anni e alla scarsità di vulnerabilità utili nei sistemi aperti verso Internet. Di conseguenza, gli hacker oggi indirizzano i loro attacchi verso gli utenti più vulnerabili, convincendoli a compiere una qualche azione che comprometta i loro sistemi. Se basta un clic per abilitare le macro, perché lanciarsi nel complicato obiettivo di trovare una vulnerabilità in un sistema operativo o browser moderno?

Ci aspettiamo anche che non ci si sposterà dal "malware fileless" per le attività post-compromissione. Dal punto di vista di un cybercriminale, quale modo migliore per evitare il rilevamento di malware se non utilizzando qualcosa che non sia malware? Ci aspettiamo che gli hacker continuino a sfruttare i LOLBins e i LOLScripts ("Living off the land Binaries/Scripts") per compromettere i sistemi e rubare/danneggiare i dati. È fondamentale che le aziende lavorino per individuare e prevenire l'uso pericoloso di questi LOLBins lavorando per fermare la compromissione iniziale e limitando l'uso di strumenti come PowerShell ovunque sia possibile.

Attacchi BEC

Sono già un problema di massa, ma gli attacchi di business email compromise (BEC) accresceranno il loro peso. Con un costo per le organizzazioni stimato in miliardi di dollari ogni anno, la frode BEC è responsabile della maggior parte delle richieste di risarcimento in tema di cyber-assicurazione e ha una barriera all'ingresso molto bassa, quindi rimarrà una forte attrazione per i cybercriminali. Di conseguenza, gli hacker lavoreranno per aumentare ulteriormente potenziale di guadagno e tasso di successo, compiendo il passo ulteriore di compromettere l'account di un utente per poi fingere di essere legittimi. L'FBI ha già attribuito al BEC la maggior parte delle perdite dovute al cybercrime e, man mano che i responsabili BEC ampliano il loro set di strumenti per

compromettere gli account cloud e i fornitori e i venditori delle organizzazioni, fermarli continuerà a essere una sfida impegnativa.

L’automazione e sicurezza

La carenza di talenti nel campo della cybersecurity è da anni una preoccupazione, con i CISO che lottano per mantenere nel tempo team completi e qualificati. L’unico modo per far sopravvivere le funzioni di sicurezza è automatizzare componenti del loro ruolo – dall’amministrazione degli account (nuovi ingressi, trasferimenti, abbandoni) all’amministrazione del firewall, fino alla creazione di metriche, al triage e agli avvisi del SOC, alle indagini DLP e altro ancora. Fino a oggi, l’automazione è stata in genere affrontata acquistando strumenti o funzionalità aggiuntive dai fornitori. Ci aspettiamo che questa situazione cambierà nel 2021, dato che l’automazione diventerà più che altro una funzione standard “in the box” per la maggior parte degli strumenti di sicurezza enterprise – cosa che molti CISO attendono ormai da tempo.

Gruppi di cybercriminali sempre più forti

I tre canali preferenziali utilizzati dai cybercriminali per il loro profitto sono BEC, EAC (email account compromise) e ransomware. Molti hacker specializzati in BEC ed EAC, tuttavia, non tendono a fungere da intermediari per i team specializzati nel ransomware, anche se dispongono dell’accesso necessario. Analogamente, gli attori di minacce focalizzati sul ransomware non tendono a utilizzare attacchi BEC ed EAC. Ci aspettiamo che questa situazione cambierà nel corso del 2021, quando i vari cybercriminali collaboreranno sempre più per creare attacchi più efficaci e raccogliere maggiori profitti. Ad esempio, potremmo vedere imprese colpite da attacchi EAC, con un accesso viene poi “venduto” a un altro

gruppo per inviare ransomware; in alternativa, il gruppo EAC potrà elevare le proprie competenze iniziando a sfruttare strumenti di ransomware disponibili in commercio. Ci attendiamo anche attacchi BEC ed EAC più avanzati.

Il prossimo anno continuerà certamente a rappresentare una sfida per i responsabili della sicurezza; tuttavia, la possibilità di fare leva su una strategia incentrata sulle persone, che protegge gli utenti attraverso i canali di comunicazione di cui hanno bisogno per lavorare, contribuirà a garantire l'efficacia delle loro contromisure.

Mancano i talenti

La pandemia ha portato a un taglio delle risorse per molte organizzazioni, compresa la spesa per la sicurezza. Speriamo di vedere nel 2021 un ritorno alla "normalità" e questo si rifletterà probabilmente nei budget per la sicurezza che torneranno ai livelli previsti. Il personale responsabile, tuttavia, non è un problema di breve termine. Infatti, i CISO continueranno a lottare per reclutare risorse per i loro team in crescita. L'offerta di posizioni remote e flessibili aiuterà organizzazioni di tutte le dimensioni, ma il problema dell'aumento degli stipendi continuerà. Di conseguenza, molte aziende più piccole e regionali si troveranno a non potersi permettere i talenti di cui hanno effettivamente bisogno, nonostante possano accedere a un bacino ancoro più diversificato costituito da lavoratori completamente remoti.

https://www.key4biz.it/cybersecurity-i-principali-trend-per-il-2021/336234/