Parler, hackerati 56,7 terabyte di dati prima della chiusura del sito

Doveva essere il momento della svolta per **Parler**, il social sovranista che piace tanto ai seguaci di Trump. E invece nell'arco di due giorni è stato quasi annientato.

Prima **Google** e **Apple** hanno rimosso l'app della piattaforma dai loro store digitali poco prima che **Amazon** staccasse la spina ai server lasciando di fatto il sito offline per tutti i seguaci di Trump e gli altri utenti iscritti.

Infine il colpo di grazia. Una ricercatrice informatica è riuscita infatti a scaricare tutto il social network, quindi ogni singolo messaggio e profilo dal portale, comprese informazioni potenzialmente incriminanti come ad esempio fotografie degli assalti al Congresso scattate il 6 gennaio, pubblicate sul sito e già cancellate poco prima che Amazon chiudesse forzatamente i battenti.

L'hacker Donk_enby

L'hacker che ha compiuto il gesto, donk_enby, una ragazza di 26 anni, è stata in grado di acquisire e archiviare quasi l'intero contenuto del sito Web, circa 56,7 terabyte, dopo che centinaia di sostenitori di Trump avevano caricato foto e video potenzialmente incriminanti di se stessi sulla piattaforma, riprese dall'interno del Campidoglio stesso durante l'assalto del 6 gennaio.

Quando le voci sull'imminente cancellazione di Parler hanno cominciato a circolare, donk_enby, che ha fatto ricerche su

Parler per mesi, ha capito che una litania di informazioni importanti sui più importanti gruppi estremisti di estrema destra d'America rischiava di essere permanentemente nascosta agli occhi del pubblico.

"Tutto ciò che abbiamo acquisito era pubblicamente disponibile sul Web, ne abbiamo semplicemente creato un'istantanea pubblica permanente", ha commentato donk_enby in un'intervista al sito Vice.com.

"Con l'FBI, le forze dell'ordine statali e locali e gli investigatori open source che cercano i responsabili dell'attacco di mercoledì, l'archivio potrebbe essere molto utile per un'intera schiera di persone", ha dichiarato Donk_emby.

"Spero che l'archivio possa essere utilizzato per ritenere le persone responsabili e per prevenire ulteriori morti", ha detto. *"Penso che alle persone dovrebbe essere consentito di avere la propria opinione fintanto che possono agire in modo civile, mercoledì abbiamo visto cosa può accadere se non lo fanno".*

La scarsa sicurezza di Parler

Usando un iPad e **Ghidra**, un software di reverse engineering progettato e rilasciato pubblicamente dalla National Security Agency, donk_enby è riuscita a sfruttare i punti deboli nel design del sito web per estrarre gli URL di ogni singolo post pubblico su Parler in ordine sequenziale, dal primo all'ultimo, permettendole di catturare e archiviare i contenuti.

Donk_enby aveva originariamente inteso acquisire dati solo dal giorno dell'acquisizione del Campidoglio, ma ha scoperto che la **scarsa costruzione e sicurezza di Parler le hanno permesso di acquisire, essenzialmente, l'intero sito web.**

Alla fine sono stati 56,7 terabyte di dati, che includevano ogni post pubblico su Parler, 412 milioni di file in tutto, inclusi 150 milioni di foto e più di 1 milione di video.

Ognuno di questi aveva metadati incorporati come data, ora e coordinate GPS: a differenza della maggior parte dei siti di social media, Parler non elimina i metadati dai media caricati dagli utenti, il che, soprattutto, potrebbe essere utile per le forze dell'ordine e gli investigatori open source.

I dati sono attualmente in fase di elaborazione e dovrebbero essere disponibili per la navigazione tra un paio di giorni, secondo donk_enby. I primi archivi di esso stanno già spuntando come file torrent e vengono condivisi su canali IRC e diversi siti git.

https://www.key4biz.it/parler-hackerati-567-terabyte-di-dati-prima-della-chiusura-del-sito/339188/

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

Ospedali italiani bersagli facili, i cyber attacchi aumentati del +81% negli ultimi due mesi

Il 2020 non sarà ricordato solo per la tremenda pandemia di **Covid-19**, ma anche per un aumento sostanziale degli **attacchi informatici alle strutture sanitarie e gli ospedali** che sono in prima linea nella battaglia contro il virus e che di fatto si stanno dimostrando bersagli facili.

I cyber attacchi agli ospedali e più in generale alle strutture sanitarie sono cresciuti del +45% a livello mondiale a novembre e dicembre 2020.

Ospedali di tutto il mondo sotto cyber attacco

Secondo i ricercatori Check Point Research, **il numero di attacchi informatici nel settore sanitario e ospedaliero è pari al doppio dell'aumento medio (+22%) dei cyber-attacchi in tutti gli altri settori industriali**.

Tali attacchi si sono verificati a novembre e dicembre 2020 soprattutto in **Europa centrale** (+145%), seguita dall'**Asia orientale** (+137%), dall'**America Latina** (+112%), dall'**Europa** (+67%) e dal **Nord America** (+37%).

Tra i principali vettori di attacco ci sono **ransomware**, **botnet**, l'esecuzione di **codici a distanza** e gli attacchi **DDoS**. Il ransomware ha mostrato il maggiore aumento e si pone come

la minaccia malware più significativa per le organizzazioni sanitarie, se confrontato con altri settori industriali.

Ospedali bersagli facili

Perché gli ospedali? Perché per i cyber criminali si tratta di bersagli facili, organizzazioni al momento sotto pressione e sotto gli occhi di tutti, che non possono fallire o sbagliare, con la vita di milioni di persone, quindi sono organizzazioni che in caso di attacco ransomware sono pronte a pagare qualsiasi somma richiesta dai cyber criminali, pur di evitare la sottrazione di dati clinici relativi ai pazienti, il blocco dei programmi di vaccinazione e dei macchinari, o la manipolazioni dei software in amministrazione o delle macchine in funzione nei reparti.

L'anno scorso, si legge nello studio, alcune reti ospedaliere in tutto il mondo sono state colpite con successo da attacchi di tipo ransomware e questo ha reso i cyber criminali ancora più motivati e fiduciosi nel buon esito dell'attacco, che è sempre finalizzato alla massimizzazione del profitto.

Italia tra i Paesi più colpiti

A livello di singoli Stati, **l'Italia è il quarto Paese al mondo ad aver subito più attacchi informatici** alle strutture sanitarie ed ospedaliere negli ultimi due mesi.

Dopo il **Canada** con un aumento di cyber attacchi sanitari del +250%, c'è la **Germania**, con un +220%, la **Spagna**, con un +100%, e quindi l'Italia, con un incremento di cyber attacchi del +81%.

In termini regionali, è **l'Europa la più colpita**, con l'Europa centrale che segna un aumento di cyber attacchi del +145%, l'Europa orientale un incremento del +87% e quella meridionale del +17%.

L’Europa nel suo complesso registra un +67%.

> *Ospedali italiani bersagli facili, i cyber attacchi aumentati del +81% negli ultimi due mesi*

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/

Cybersecurity trend 2021: sarà l'anno di Ransomware e "fileless malware"

Dopo un anno in cui la pandemia da Covid-19 ha sconvolto il modo di vivere, lavorare e socializzare in tutto il mondo, è probabile che nel 2021 le maggiori minacce saranno rappresentate da ransomware e fileless malware. È quanto emerge dall'ultimo Report pubblicato da ESET.

Il documento analizza le previsioni degli esperti di cybersecurity, rivelando le sfide chiave che potrebbero avere un impatto su consumatori e aziende nel 2021.

Trend #1 Il futuro del lavoro

A***bbracciare una nuova realtà***

L'emergenza sanitaria da pandemia ha portato all'implementazione di massa del lavoro da remoto, la cui efficacia dipende fortemente dalla tecnologia. La possibilità di lavorare da casa ha portato benefici ai dipendenti, ma ha anche messo a rischio di attacchi le reti aziendali.

Jake Moore, Security Specialist di ESET, ha commentato "*Abbiamo tutti compreso che il lavoro da remoto è un vantaggio per le aziende, anche se non credo che in futuro potremo continuare a lavorare in smart working per l'intera settimana. Molti lavoratori in tutto il mondo migreranno naturalmente e senza sforzo verso le modalità che migliorano il proprio lavoro e quello delle loro aziende. Via via che il processo di digitalizzazione evolve nella vita professionale e domestica, gli attacchi informatici diventano una minaccia persistente e*

le imprese devono dotarsi di team e sistemi IT resilienti per evitare le conseguenze economiche e reputazionali legati ai nuovi malware”.

Trend #2 Ransomware con colpo di scena finale

Richieste di riscatto per salvare i dati

Gli hacker che utilizzano i malware ransomware per estorcere denaro stanno alzando il tiro. Esfiltrazione ed estorsione sono tecniche non nuove, ma certamente in crescita.

Tony Anscombe, Chief Security Evangelist dell’azienda ha dichiarato: “*Le aziende si stanno evolvendo, implementando tecnologie che ostacolano gli attacchi e creando processi di backup e ripristino resilienti, perciò i malintenzionati hanno bisogno di un ‘Piano B’ per poter monetizzare la propria attività illecita. La capacità di risposta alle minacce o i processi di ripristino potrebbero però non essere più sufficienti a respingere un criminale informatico che chiede il pagamento di un riscatto. Cambiare la tecnica di attacco può offrire ai cybercriminali una maggiore possibilità di ritorno economico. Questa è una tendenza che, purtroppo, vedremo fiorire nel 2021*”.

Trend #3 Oltre la prevenzione

Aggiornarsi alle evoluzioni delle minacce informatiche

Negli ultimi anni, i criminali informatici hanno optato per l’utilizzo di tecniche sempre più complesse per diffondere attacchi mirati.

Qualche tempo fa la Security Community ha iniziato a parlare di “***fileless malware***” che si basano sui tool e sui processi del sistema operativo sfruttandoli a scopi dannosi. Queste

tecniche hanno preso forza di recente e sono state impiegate in varie campagne di cyberspionaggio da diversi cybercriminali, principalmente per colpire obiettivi di alto profilo come gli Enti Governativi.

Camilo Gutiérrez Amaya, Senior Security Researcher del Gruppo ha osservato: "*Le minacce fileless si sono evolute rapidamente e prevediamo che queste tecniche nel 2021 verranno utilizzate in attacchi sempre più complessi e su larga scala. Ciò mostra la necessità per i team di sicurezza di sviluppare processi che sfruttano strumenti e tecnologie non solo per impedire al codice dannoso di compromettere i sistemi informatici, ma che abbiano anche capacità preventiva di rilevamento e risposta agli attacchi*".

Per maggiori informazioni sulle tendenze che avranno un impatto globale nel 2021 consultare il Rapporto "***Cybersecurity Trends 2021: Staying secure in uncertain times***".

Cybersecurity trend 2021: sarà l'anno di Ransomware e "fileless malware"

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/