Attacco phishing in Germania: rubati milioni di euro dai contributi per l'emergenza Covid

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

I pirati informatici hanno raccolto i dati personali degli aventi diritto ai sussidi nella regione del Nord Reno Westfalia e hanno dirottato milioni di euro sui loro conti.

Con l'emergenza coronavirus, ci si poteva aspettare una tregua da parte dei cyber-criminali. Niente da fare: se l'**FBI** segnala addirittura un aumento di 4 volte dell'attività dei pirati informatici, anche in Europa i truffatori si stanno dando parecchio da fare.

L'attacco più clamoroso ha preso di mira l'amministrazione della regione tedesca del **Nord Reno Westfalia**, che nei giorni scorsi ha avviato un programma di sussidi pubblici per sostenere i cittadini in difficoltà a causa del blocco delle attività sul territorio.

I responsabili IT della regione tedesca, però, hanno organizzato la procedura in maniera per lo meno inadeguata. **In pratica, il sito Internet dedicato alla richiesta del contributo prevedeva esclusivamente la compilazione di un modulo, senza verifiche ulteriori**.

Ad approfittarne è stato un gruppo di pirati informatici che hanno messo in piedi un classico schema di phishing attraverso il quale avrebbero rubato milioni di euro all'amministrazione del Nord Reno Westfalia.

I cyber-criminali, in pratica, hanno messo in piedi un clone del sito ufficiale e hanno usato una campagna di spam via posta elettronica per attirare quanti più cittadini potessero, registrando i loro dati.

Hanno poi usato queste informazioni per compilare le richieste sul sito legittimo, indicando però per i versamenti dei conti correnti sotto il loro controllo.

Secondo le autorità tedesche, sui 360.000 pagamenti autorizzati dall'amministrazione del land, ben 4.000 sarebbero stati fraudolenti. **Dal momento che la somma una tantum versata dal governo tedesco varia tra i 9.000 euro per i lavoratori autonomi e i 25.000 euro destinati invece alle aziende con più di 50 dipendenti, staremmo parlando di un danno complessivo tra i 31,5 e i 100 milioni di euro**.

Insomma: un colpo clamoroso, che poteva privare migliaia di cittadini di un sostegno fondamentale in un momento di crisi che non è solo sanitario, ma anche economico.

Per fortuna le autorità procederanno a erogare i sussidi anche ai cittadini truffati, verificando questa volta che il conto corrente indicato corrisponda a quello utilizzato per l’ultimo pagamento delle tasse.

Condividi l’articolo

Nuova campagna di truffe per i buoni spesa gratuiti Operazione ICEBUCKET: truffa in grande stile sulle pubblicità

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/20/attacco-phishing-in-germania-rubati-i-contributi-per-lemergenza-coronavirus/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-phishing-in-germania-rubati-i-contributi-per-lemergenza-coronavirus

---

Operazione ICEBUCKET: truffa in grande stile sulle pubblicità

Apr 17, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, RSS 0

I cyber-criminali hanno messo in piedi un sistema che ha permesso di incassare proventi per pubblicità visualizzate su una rete di false Smart TV.

Una gigantesca truffa che ha preso di mira il sistema di collocamento delle pubblicità online e ha permesso ai suoi autori di incassare enormi quantità di compensi fraudolenti. L'operazione **ICEBUCKET**, spiegano gli esperti di **White Ops**, potrebbe essere la più grande truffa di questo genere mai individuata.

Come spiegano nel loro report, i pirati informatici sono riusciti a creare una gigantesca rete di falsi dispositivi che imitavano il comportamento di reali utenti per visualizzare pubblicità che venivano regolarmente pagate ma, in realtà, non venivano viste da nessuno.

Per capire lo schema della truffa, però, è necessario fare un passo indietro per contestualizzarla all'interno del meccanismo di vendita delle pubblicità online basate sul concetto di "programmatic".

Da tempo, la distribuzione delle pubblicità online viene gestita attraverso sistemi automatici che "piazzano" gli spot quasi in tempo reale, utilizzando una serie di parametri come la posizione geografica degli utenti che visualizzeranno i video, il loro profilo e altri parametri.

Lo schema prevede una forma di intermediazione, gestita attraverso la tecnologia **Server-Side Ad Insertion (SSAI)** che permette di distribuire i contenuti pubblicitari con una maggiore efficienza, soprattutto quando è diretta a dispositivi mobili o Smart TV.

I cyber-criminali che hanno orchestrato ICEBUCKET sono riusciti a inserirsi in questo schema, ingannando le piattaforme che comprano spazi pubblicitari.

In pratica, i truffatori riuscivano a proporre spazi pubblicitari disponibili facendo in modo che la richiesta provenisse da server SSAI affidabili. **In realtà, però, si trattava di false richieste, che facevano riferimento a dispositivi inesistenti**.

Per mettere in piedi questo sistema, i pirati avrebbero usato un'infrastruttura estremamente complessa, composta da 1.000 user agent differenti, 2 milioni di falsi indirizzi IP da oltre 30 nazioni (il 99% negli USA) e circa 1.700 server SSAI dislocati in 9 paesi diversi.

Per aumentare i loro guadagni, gli autori della truffa hanno scelto di "impersonare" principalmente Smart TV. Nel mercato pubblicitario, infatti, questi dispositivi sono considerati più "pregiati" e garantiscono di conseguenza maggiori ricavi.

Secondo i ricercatori di White Ops, lo schema ICEBUCKET avrebbe permesso, nei momenti di punta, di **vendere quasi 2 miliardi di inserzioni fraudolente al giorno**. L'impatto, nel mese di gennaio, sarebbe stato tale da assorbire il 28% del mercato pubblicitario basato su programmatic.

Insomma: una truffa di dimensioni clamorose, che è stata bloccata soltanto dopo settimane in cui i pirati sono riusciti ad agire indisturbati e, soprattutto, a nascondere le loro tracce con un'abilità davvero fuori dal comune.

Condividi l’articolo

Zoom: il punto della situazione sulla sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/17/operazione-icebucket-truffa-in-grande-stile-sulle-pubblicita/?utm_source=rss&utm_medium=rss&utm_campaign=operazione-icebucket-truffa-in-grande-stile-sulle-pubblicita

---

Zoom: il punto della situazione sulla sicurezza

Apr 16, 2020 Marco Schiaffino Gestione dati, Hacking, In evidenza, News, Privacy, RSS, Vulnerabilità 0

Tra allarmi, bufale e zoombombing, il software di videoconferenza è al centro delle cronache. E spuntano zero-day in vendita per 500.000 dollari.

È passato da 10 a 200 milioni di utenti in un paio di settimane e i problemi di sicurezza non sono mancati. Capire quale sia l’attuale livello di affidabilità di **Zoom**, però, è difficile anche per gli addetti ai lavori. Proviamo a fare il punto della situazione sulla base di quanto è emerso fino a

ora.

Il rispetto della privacy

Gli allarmi per la possibilità che la stessa azienda con sede a San Jose rastrellasse informazioni sensibili attraverso la sua piattaforma, addirittura **usando le trascrizioni delle videoconferenze**, sono circolate per qualche giorno ma si sono dimostrate infondate.

Come abbiamo spiegato in questo articolo, le condizioni di utilizzo di Zoom prevedono esplicitamente che non sia raccolta alcuna informazione dai dati trasmessi e ricevuti nelle conversazioni. Il riferimento a una raccolta di dati a scopo di marketing si riferivano infatti al sito (e ai soliti cookie) e non alla piattaforma.

Qualche polemica è sorta invece riguardo alla possibilità che alcune connessioni passassero per i datacenter situati in Cina. Un fatto che ha sollevato preoccupazioni soprattutto tra gli utenti che abitano in paesi vicini (Taiwan ha addirittura messo al bando il software) e che temono che i loro dati possano essere intercettati dalle autorità di Pechino.

Dal 18 aprile, l'azienda permetterà ai suoi utenti con licenza a pagamento di impostare il routing dei dati in modo da avere la certezza di evitare "passaggi a rischio" come quelli attraverso i datacenter cinesi.

Zoom, è bene ricordarlo, non utilizza un sistema di crittografia end to end, ma una "semplice" crittografia TLS come quella usata da tutte le connessioni su protocollo HTTPS. La preoccupazione per un'eventuale intercettazione, quindi, non completamente infondata e rende il suo utilizzo sconsigliabile per comunicazioni particolarmente riservate.

Riservatezza e impostazioni

I problemi non sono mancati, invece, nella gestione delle videoconferenze. Soprattutto nelle prime settimane di “boom” nell’utilizzo del software, la sua architettura ha mostrato limiti piuttosto evidenti.

La procedura predefinita per l’avvio di una sessione di Zoom prevedeva infatti la creazione di una URL che consentiva il collegamento a chiunque la conoscesse. Il risultato è stato la nascita del fenomeno del cosiddetto **zoombombing**, cioè la pratica di fare irruzione in videoconferenze per disturbarle con interventi inappropriati che, nella maggior parte dei casi, hanno avuto carattere goliardico.

A spingere il fenomeno è stato, più che altro, l’utilizzo di Zoom per gestire la didattica a distanza nel periodo di distanziamento sociale. Molti studenti, infatti, hanno pensato di approfittare della situazione per giocare qualche scherzo agli insegnanti, organizzando anche dei veri e propri canali dedicati su Discord per distribuire i collegamenti alle videoconferenze.

Dalle parti di Zoom hanno reagito modificando le impostazioni predefinite, introducendo l’uso di una password come procedura

“normale” per la creazione della conferenza e abilitando, allo stesso modo, la funzione della waiting room, che lascia in attesa i partecipanti fino a quando l’host della conferenza non ne approva la partecipazione.

Furto di credenziali

Tra gli allarmi circolati in questi giorni, c’è anche quello che vedrebbe un massiccio attacco hacker che avrebbe portato al furto di **500.000 credenziali di utenti Zoom che sono finite in vendita sul Dark Web**.

Se la notizia è stata confermata da numerose società di sicurezza, le conclusioni tratte da alcuni organi di stampa riguardo una presunta vulnerabilità di Zoom sono invece ben poco fondate.

Secondo gli esperti che hanno individuato i database in questione, infatti, si tratterebbe di username e password ottenuti attraverso tecniche di credential stuffing, cioè attraverso l’uso di combinazioni di username e password che gli utenti hanno utilizzato anche in altri servizi e che erano già in circolazione nei bassifondi di Internet.

Il tema della sicurezza, però, è qualcosa con cui dalle parti di Zoom hanno deciso di prendere sul serio. Per farlo, l’azienda si è rivolta ad **Alex Stamos**, esperto di sicurezza che ha lavorato in passato con **Yahoo!** (in uno dei periodi meno felici dell’azienda statunitense) e con **Facebook**.

Il suo intervento potrà consentire qualche correzione relativa ai rischi dell’uso di link all’interno della chat (abbiamo parlato dei rischi in questo articolo) e a una più complessiva revisione dell’architettura del software che sembra ancora piuttosto debole.

Le falle di sicurezza

Tutto bene quindi? No. Perché qualche vulnerabilità "reale" Zoom ce l'ha. Le uniche di cui si conoscono i dettagli (qui il pirotecnico report che le illustra) riguardano la possibilità di un attacco locale su sistemi macOS.

Il vero allarme, però, è arrivato oggi con la notizia riportata da **Motherboard** riguardante la disponibilità di **un exploit zero-day che sfrutterebbe una vulnerabilità critica del client per Windows**. Il bug, di cui non si conoscono i dettagli tecnici, consentirebbe di avviare l'esecuzione di codice in remoto. **Tradotto: permetterebbe di usare Zoom come vettore per un attacco malware**.

Stando a quanto viene riportato nell'articolo, l'exploit sarebbe in vendita al prezzo di **500.000 dollari** su quelli che possiamo considerare "mercati informali" del Dark Web. Una quotazione che non stupisce più di tanto, visto che piattaforme "legali" che si occupano di compravendita di

exploit come la famigerata **Zerodium** arrivano a offrire fino a 2,5 milioni di dollari per gli exploit sui sistemi e software più diffusi.

Sempre stando alle fonti contattate da Motherboard, esisterebbe poi un altro exploit, relativo però al client per macOS. Insomma: Alex Stamos e i suoi colleghi si trovano ad affrontare una situazione tutt'altro che facile. Il suggerimento, per il momento, è quello di eseguire regolarmente gli aggiornamenti di Zoom per avere la certezza di utilizzare la versione più sicura del software.

Condividi l'articolo

EDP colpita dal ransomware RagnarLocker. Riscatto da 10 milioni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/16/zoom-il-punto-della-situazione-sulla-sicurezza/?utm_source=rss&utm_medium=rss&utm_campaign=zoom-il-punto-della-situazione-sulla-sicurezza

---

EDP colpita dal ransomware

RagnarLocker. Riscatto da 10 milioni

Apr 15, 2020 Marco Schiaffino Attacchi, In evidenza, Leaks, Malware, News, RSS 0

L'azienda petrolifera Energias de Portugal è rimasta vittima di un attacco che ha bloccato i suoi sistemi. I pirati vogliono 1.580 Bitcoin.

Si tratta probabilmente del tentativo di estorsione più ambizioso nella storia della pirateria informatica. La vittima è **Energias de Portugal** (EDP), multinazionale del settore energetico con sede a **Lisbona**. Il malware usato per mettere K.O. i sistemi dell'azienda, con lo scopo di chiedere un riscatto "monstre" di quasi 10 milioni di euro, è invece **RagnarLocker**.

A riportarlo è **Bleeping Computer**, che in un articolo riassume i tratti principali della vicenda come riportati dai ricercatori di **MalwareHunterTeam**.

La richiesta dei pirati informatici (**1.580 Bitcoin, pari a circa 9,9 milioni di euro**) dimostra, ancora una volta, il motivo per cui i cyber-criminali negli ultimi mesi si stiano concentrando sempre più spesso sulle aziende.

I pirati informatici, infatti, sanno che le imprese possono permettersi di pagare riscatti decisamente più sostanziosi rispetto agli utenti privati. Soprattutto, il meccanismo estorsivo può sfruttare elementi diversi rispetto alla semplice minaccia di "bloccare" i file.

Nel caso di EDP, infatti, gli autori dell’attacco hanno pubblicato un messaggio online annunciando di aver sottratto la bellezza di 10 TB di dati dai sistemi dell’azienda. L’elemento su cui contano di più i cyber-criminali, però, non è tanto il ripristino dei sistemi, quanto la volontà dei dirigenti di evitare un leak di informazioni che potrebbe danneggiare l’impresa.

Non è un caso che nei loro messaggi, gli autori dell’attacco minaccino esplicitamente di fornire i dati che hanno rubato agli organi di stampa, sottintendendo che all’interno dei documenti sottratti ci siano informazioni compromettenti per EDP. Il tema, in pratica, è quello del **danno reputazionale** che l’azienda potrebbe soffrire.

Per garantire migliore efficacia alla loro strategia, i pirati hanno pubblicato una parte dei dati contenenti informazioni personali riguardanti gli impiegati dell’azienda. Una mossa che ha lo scopo di dimostrare alla vittima che il breach (e la minaccia) è reale.

Condividi l’articolo

Zoom: il punto della situazione sulla sicurezza Falla critica in VMware: aggiornare di corsa!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/15/edp-colpita-dal-ransomw

are-ragnarlocker-riscatto-da-10-milioni/?utm_source=rss&utm_medium=rss&utm_campaign=edp-colpita-dal-ransomware-ragnarlocker-riscatto-da-10-milioni

---

Falla critica in VMware: aggiornare di corsa!

Apr 14, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità interessa il sistema di gestione centralizzata di VMware e consentirebbe di accedere a tutte le informazioni conservate sui sistemi.

Non accade spesso che una vulnerabilità ottenga un rating di 10 su 10. Quando succese, per gli amministratori IT significa una sola cosa: grossi guai. Se il bug in questione affligge un software diffuso come **VMware**, poi, la situazione può essere senza dubbio definita critica.

La segnalazione, pubblicata dalla stessa azienda con un documento di approfondimento sul suo sito, riguarda un bug (CVE-2020-3952) all'interno di **VMware Directory Service (vmdir)** e può avere conseguenze devastanti. Se sfruttata, infatti, consentirebbe a un pirata informatico di accedere liberamente a tutte le informazioni memorizzate sui sistemi virtuali.

Il componente in quesitone, infatti, fa parte di **vCenter Server**, il sistema di gestione centralizzato di VMware che gestisce, tra le altre cose, i certificati per l'accesso che permettono di controllare in massa tutte le installazioni.

Insomma: violare vmdir significa in pratica avere il controllo assoluto.

La falla di sicurezza permette di aggirare il sistema di autenticazione e, secondo gli sviluppatori di VMware, non è possibile correggerla agendo sulle impostazioni del software. L'unica soluzione, in buona sostanza, è applicare la patch.

La parte più problematica, a quanto si capisce, è capire se la propria installazione è vulnerabile o meno all'attacco. Il bug è presente sulle versioni di vCenter Server aggiornate alla versione 6.7 da installazioni precedenti, mentre le "nuove" installazioni (quelle cioè eseguite direttamente con la versione 6.7) sarebbero sicure.

Gli esperti di VMware, in ogni caso, consigliano di verificare i log di sistema per controllare se il bug sia presente ed eseguire l'aggiornamento il prima possibile. Considerata la diffusione del software di virtualizzazione, infatti, l'impatto di un eventuale exploit in grado di sfruttare la vulnerabilità potrebbe essere devastante.

Condividi l’articolo

Ecco DDG: la prima botnet peer to peer

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/14/falla-critica-in-vmware-aggiornare-di-corsa/?utm_source=rss&utm_medium=rss&utm_campaign=falla-critica-in-vmware-aggiornare-di-corsa

---

Ecco DDG: la prima botnet peer to peer

Apr 10, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

I pirati informatici che la gestiscono hanno sviluppato un sistema di comunicazione tra le macchine infette che la rende estremamente resistente.

Fino a qualche mese fa, la botnet **DDG** veniva considerata dagli esperti come qualcosa di assolutamente “normale”. I suoi autori, infatti, la utilizzavano per installare crypto-miner su server vulnerabili e controllavano la sua attività attraverso un classico collegamento a un server Command and

Control.

Le cose, però, sono cambiate lo scorso febbraio. I ricercatori di **Netlab 360** si sono infatti accorti che i cyber-criminali hanno introdotto un cambiamento significativo nell'architettura della rete, abilitando un sistema di comunicazione peer to peer tra le macchine infette.

Come spiegano nel loro report (consigliamo di usare un sistema di traduzione verso l'inglese per ottenere un testo abbastanza fedele all'originale) i pirati informatici hanno sviluppato un protocollo proprietario che consente a ogni dispositivo infetto di comunicare con altri 200 bot della rete.

In questo modo, DDG è in grado di sopravvivere anche nel caso in cui il server C&C venisse momentaneamente bloccato e il malware può garantire la sua diffusione e persistenza.

Quello messo in piedi, spiegano i ricercatori, è in realtà un sistema ibrido, in cui le comunicazioni P2P servono come elemento di ridondanza rispetto ai server C&C.

Da un punto di vista tecnico, DDG si diffonde utilizzando un sistema di brute forcing basato su attacchi a dizionario, che fanno leva sull'utilizzo di password "deboli" per l'accesso ai server.

Il database utilizzato dal malware, che viene offuscato attraverso un sistema di crittografia basato su algoritmo AES, comprenderebbe la bellezza di 17.907 password.

Secondo i ricercatori, che sottolineano anche la presenza di un sistema di proxy utilizzato per offuscare le comunicazioni tra i peer, le caratteristiche di DDG permetterebbero alla botnet di diffondersi in maniera inesorabile, forse lenta, ma inesorabile.

Condividi l'articolo

La botnet dark_nexus fa strage di dispositivi IoT

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/10/ecco-ddg-la-prima-botnet-peer-to-peer/?utm_source=rss&utm_medium=rss&utm_campaign=ecco-ddg-la-prima-botnet-peer-to-peer

---

La botnet dark_nexus fa strage di dispositivi IoT

Apr 09, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Utilizza un codice copiato da altre botnet, ma i suoi autori hanno introdotto funzionalità e strumenti di attacco innovativi che la rendono più robusta.

La si potrebbe definire "evoluzione della specie". La comparsa della botnet **dark_nexus**, infatti, rappresenta un nuovo sviluppo nel campo dei malware che prendono di mira i dispositivi IoT come **Mirai** e **Qbot**.

Il malware, che secondo i ricercatori di **Bitdefender** è stato sviluppato partendo proprio dal codice del celebre Mirai, è stato ripetutamente aggiornato tra dicembre 2019 e aprile 2020, introducendo una serie di funzionalità che lo rendono più potente e robusta rispetto ai suoi predecessori.

In particolare, si legge nel report, dark_nexus usa due moduli (uno sincrono e uno asincrono) per sfruttare exploit e tecniche di **credential stuffing** che gli consentono di prendere il controllo dei dispositivi attraverso il collegamento **Telnet**.

La botnet utilizza poi un payload estremamente specializzato, che viene scelto sulla base delle caratteristiche del dispositivo compromesso. **I ricercatori hanno individuato ben 12 varianti, ognuna delle quali è programmata per ottimizzare il funzionamento del malware sullo specifico modello di processore installato**.

Gli autori di dark_nexus hanno, come obiettivo, quello di utilizzare le macchine compromesse per portare attacchi DDoS, ma hanno scelto di **adottare un sistema di offuscamento** che altera la trasmissione dei dati in modo che a una prima analisi sembri normale traffico generato da un browser.

Secondo i ricercatori, le dimensioni della botnet sarebbero ancora piuttosto limitate. **Il numero di dispositivi infetti sarebbe infatti di 1.372 bot, principalmente distribuiti tra Brasile, Cina, Sud Corea e Tailandia**.

Le caratteristiche di dark_nexus, così come indica anche la frequenza degli aggiornamenti, sono però tali da far pensare che si tratti di un processo in piena fase di sviluppo.

Il rischio, insomma, è che la botnet raggiunga nel giro di qualche settimana dimensioni decisamente maggiori e possa trasformarsi in un problema pari, per impatto sulla rete globale, a quello che ha rappresentato Mirai per lungo tempo.

Condividi l’articolo

Ancora xHelper: il trojan per Android è immortale

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/09/la-botnet-dark_nexus-fa-strage-di-dispositivi-iot/?utm_source=rss&utm_medium=rss&utm_campaign=la-botnet-dark_nexus-fa-strage-di-dispositivi-iot

---

Ancora xHelper: il trojan per Android è immortale

Apr 08, 2020 Marco Schiaffino In evidenza, Malware, News, RSS, Scenario 0

Il malware è in circolazione dall'anno scorso e non sembra rallentare. Gli esperti: "gli utenti continuano a installare app da siti non affidabili".

La proliferazione di app malevole per Android non è una notizia e la continua comparsa di nuovi malware è qualcosa a cui ormai ci siamo abituati. Ne esiste, però, una categoria particolare: quelli che sembrano non avere nessuna intenzione di sparire anche dopo l'individuazione da parte delle società di sicurezza e l'estromissione dai market ufficiali.

Il caso di **xHelper**, illustrato dai ricercatori di **Kaspersky** in un post sul blog della società di sicurezza, è emblematico. Il trojan per Android, infatti, è in circolazione da quasi un anno.

La tecnica di distribuzione utilizzata dai pirati informatici è estremamente semplice: il malware è infatti proposto come

un’app per la manutenzione del sistema e l’ottimizzazione delle prestazioni.

In realtà, tra le pieghe del codice si nascondono una serie di comandi che avviano il download e l’installazione di una serie di applicazioni malevole, compreso il trojan **Triada**.

SI tratta di una strategia che i ricercatori definiscono “a matriosca” e che sfrutta un trucchetto molto particolare: la cartella che contiene gli eseguibili viene collegata al file *install-recovery.sh* assegnando loro l’attributo “immutabile”. **In pratica, I file non possono essere cancellati attraverso le ordinarie procedure e, in alcuni casi, nemmeno con un reset alle condizioni di fabbrica**.

Molti esemplari di xHelper risultano infatti essere stati scaricati da malware preinstallati nei firmware dei telefoni, soprattutto di modelli a basso costo.

A parte questi casi limite come quelli citati, la persistenza di xHelper sembra però essere dovuta all’abitudine da parte degli utenti di ostinarsi a installare applicazioni “gratuite” offerte sulle pagine di siti di dubbia affidabilità.

Insomma, secondo i ricercatori Kaspersky siamo di fronte al solito meccanismo per cui il tentativo di risparmiare qualche euro (vista la diffusione geografica di xHelper sarebbe forse meglio parlare di rubli) si trasforma in un disastro.

Condividi l’articolo

Attacco a Email.it: 600.000 account in vendita sul Dark Web

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/08/ancora-xhelper-il-trojan-per-android-e-immortale/?utm_source=rss&utm_medium=rss&utm_campaign=ancora-xhelper-il-trojan-per-android-e-immortale

---

Attacco a Email.it: 600.000 account in vendita sul Dark Web

Apr 07, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, News, Privacy, RSS 0

I pirati informatici avrebbero tentato un’estorsione ai danni del provider e, dopo il rifiuto, hanno messo in vendita i dati sottratti.

Un clamoroso leak di dati ai danni di **Email.it**, provider di posta italiana che avrebbe subito un colossale data breach in cui sarebbero coinvolti più di **600.000 account di posta elettronica**.

La notizia prende le mosse da un tweet pubblicato dai presunti hacker, che avrebbero messo in vendita il database contenente le informazioni riguardanti le caselle email e 5 terabyte di contenuti estratti dai datacenter, che conterrebbero messaggi e allegati inviati attraverso il servizio di posta elettronica.

Stando a quanto scrivono i pirati, l’attacco avrebbe avuto luogo la bellezza di due anni fa e avrebbe permesso ai cyber criminali di “installarsi” nei sistemi di Email.it e accedere tranquillamente ai dati conservati senza che gli amministratori si accorgessero di nulla.

Peggio ancora: sul sito del **NoName Hacking Group** (raggiungibile solo nel Dark Web) i pirati informatici sostengono che Email.it abbia conservato le password degli account in chiaro (senza alcuna protezione crittografica) nonostante sul sito dell’azienda sia chiaramente indicato l’utilizzo di un sistema di crittografia “forte” per proteggere i dati degli utenti.

Secondo quanto scrivono gli hacker, l’intrusione risalirebbe al 1 gennaio 2018 e la situazione avrebbe vissuto un’escalation qualche settimana fa, quando i pirati hanno cercato di estorcere del denaro a Email.it.

L’azienda, però, avrebbe rifiutato di pagare e avrebbe tentato, stando a quanto si legge sul sito dei cyber criminali, di risolvere il problema senza darne comunicazione alcuna né alle autorità, né ai suoi utenti.

Un comportamento che, se confermato, potrebbe avere conseguenze gravissime per l'azienda, che rischia una salatissima multa ai sensi del GDPR.

Ora i pirati **hanno messo in vendita tutti i dati che hanno sottratto al datacenter**, relativi a 600.000 account di posta gratuita gestita da Email.it a prezzi che variano dagli 0,5 ai 3 Bitcoin, equivalenti a circa 3.000 – 20.000 euro.

Condividi l'articolo

Il software di supporto HP per Windows è un colabrodo

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/07/attacco-a-email-it-600-000-account-in-vendita-sul-dark-web/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-a-email-it-600-000-account-in-vendita-sul-dark-web

---

Il software di supporto HP per Windows è un colabrodo

Apr 06, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una pioggia di vulnerabilità individuate nel HP Support Assistant mettono a rischio i sistemi. E alcune non sono state ancora corrette…

Guardando alla cronaca, sembra proprio che i software per l'aggiornamento sviluppati dai produttori di PC, sotto il profilo della sicurezza, siano una categoria particolarmente "a rischio".

L'ultima segnalazione riguarda **HP Support Assistant**, che viene fornito come programma preinstallato sui dispositivi dell'azienda statunitense e fornsice funzionalità per una forma di assistenza "fai da te".

Come spiega in un post sul suo blog il ricercatore di sicurezza **Bill Demirkapi**, il software contiene 10 falle di sicurezza di gravità variabile, che passano dalla possibilità di elevare i privilegi sul sistema all'esecuzione di codice in remoto sulla macchina.

[embedded content]
Questi ultimi, illustrati nel video pubblicato dallo stesso ricercatore su **YouTube**, sono naturalmente i più gravi e quelli che, fortunatamente, HP ha corretto dopo la segnalazione di Demirkapi. **Secondo il ricercatore, però, l'intervento degli sviluppatori non è stato completamente risolutivo**.

Due vulnerabilità relative all'elevazione dei privilegi di amministrazione, infatti, sarebbero rimaste scoperte e una delle patch, anche se rilasciata, non avrebbe sortito il risultato sperato.

Si tratta, nel dettaglio, di una falla di sicurezza che riguarda il controllo del collegamento a Internet e dell'affidabilità del file scaricato per l'aggiornamento. La patch sviluppata da HP, spiega il ricercatore, si limita a introdurre un sistema di verifica dell'host a cui punta il collegamento, lasciando aperta però la possibilità di un attacco **Man in The Middle** che permetterebbe comunque di portare un attacco.

Secondo Demirkapi, in ogni caso, la soluzione migliore è quella di disinstallare HP Support Assistant. Una logica condivisibile visto che l'aggiornamento risolverebbe alcune delle vulnerabilità, ma non tutte.

Condividi l'articolo

Microsoft al lavoro per risolvere 25 bug di Windows

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/06/il-software-di-supporto-hp-per-windows-e-un-colabrodo/?utm_source=rss&utm_medium=rss&utm_campaign=il-software-di-supporto-hp-per-windows-e-un-colabrodo