Attacco al circuito Electrum: hacker intascano più di 750.000 dollari

Dic 28, 2018 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 0

Hanno sfruttato una debolezza del sistema per indurre gli utenti a scaricare un client taroccato. E non è detto che sia finita…

Colpo grosso ai danni del circuito **Electrum**. Come riporta ZDNet, ignoti hacker sarebbero riusciti a dirottare le transazioni in cripto-valuta sui loro conti per un valore superiore a 750.000 dollari.

L'attacco, che si è protratto per una settimana, ha sfruttato una debolezza intrinseca del circuito Electrum. Il sistema per la gestione della cripto-valuta si basa infatti su **un sistema client-server completamente aperto**.

In particolare, il sistema prevede che chiunque possa usare il sorgente per mettere online il suo server personale, che verrà utilizzato anche da altri utenti nelle transazioni.

Anche se il sistema è sufficientemente "blindato" per evitare attività malevole, i pirati informatici hanno trovato un modo per sfruttare questa architettura a loro vantaggio.

Nel dettaglio, gli hacker hanno sfruttato la funzione che consente di **visualizzare messaggi sotto forma di pop-up ai client che si connettono al server**.

Dopo aver messo online qualche decina di server sotto il loro controllo, hanno iniziato a inviare un messaggio in cui si

avvisava l’utente connesso che la transazione non poteva essere portata a termine perché il suo client non era aggiornato, indicando anche **un link per scaricare e installare la nuova versione**.

Il collegamento, però, non puntava a un indirizzo legittimo ma a un repository su **GitHub** con una versione “taroccata” del wallet, programmata per eseguire transazioni che trasferivano tutti i fondi presenti sul contro verso il wallet dei pirati informatici.

L’unico elemento che avrebbe potuto mettere sul chi va là gli utenti vittima dell’attacco era il fatto che al momento dell’installazione **il software chiedeva una verifica attraverso il sistema di autenticazione a due fattori, che normalmente viene usata solo per autorizzare una transazione**. Chi ha fornito la conferma si è trovato il conto svuotato.

Risultato: tra il 20 e il 27 dicembre sul conto dei cyber-criminali sono arrivati più di **200 Bitcoin**, che al cambio attuale corrispondono a **più di 750.000 dollari**.

Gli sviluppatori del circuito Electrum, una volta ricevuta la segnalazione, hanno come prima cosa distribuito un

aggiornamento per **impedire la visualizzazione di messaggi in HTML**, in modo che eventuali link all'interno dei messaggi non possano essere nascosti.

Una soluzione temporanea e ben poco efficace, visto che **alcuni utenti hanno comunque scaricato il client infetto copiando e incollando il link nel loro browser**, senza fare troppo caso al fatto che il collegamento puntasse a un indirizzo diverso da quello del sito ufficiale.

Ora **l'installer infetto è stato rimosso da GitHub**, ma è improbabile che i pirati si fermino solo per questo. Il vero problema, infatti, è che ci sono ancora decine di server sotto il controllo degli hacker.

Please follow and like us:

WannaCry è inattivo, ma ci sono ancora milioni di computer infetti Anche l'India fa una legge per intercettare i dati su Internet

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/28/attacco-al-circuito-electrum-hacker-intascano-piu-di-750-000-dollari/

Anonymous festeggia il Natale violando i siti di ASL e ospedali

Dic 27, 2018 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, News, Privacy, RSS 0

Gli hacktivist hanno fatto strage dei sistemi informatici nel settore sanitario. "Chi dovrebbe trattare con cura i nostri dati non fa il lavoro per cui viene pagato".

Un modo costruttivo per passare il tempo durante le feste di Natale? Gli hacktivist di **Anonymous Italia** l'hanno trovato avviando una campagna di attacchi nei confronti di numerosi siti Internet di **Aziende Sanitarie Locali** e strutture ospedaliere italiane. **L'obiettivo è sempre il solito: dimostrare che i dati dei cittadini italiani sono gestiti in maniera inadeguata**.

La "rivendicazione" dell'attacco è stata pubblicata sul blog ufficiale di Anonymous Italia, accompagnata da un fotomontaggio in cui gli hacktivist si sono divertiti a

reinterpretare il presepe inserendo personaggi della politica italiana. La stessa immagine è comparsa su alcuni dei siti violati.

Nel comunicato, gli hacker puntano il dito contro un sistema sanitario che, oltre a dover garantire cure mediche e salute del territorio, dovrebbe **proteggere le informazioni personali dei pazienti**. “Chi ci governa, e chi dovrebbe trattare con cura i nostri dati/privacy, non fa il lavoro per cui viene profumatamente pagato” chiosano sul loro blog.

L’azione, si legge sul blog, è stata portata insieme a gruppi differenti (e piuttosto conosciuti nel nostro paese) come **LulzSecIta** e **AntiSecIta**, che da sempre si riconoscono in quella “galassia informale” che siamo abitutati a chiamare Anonymous.

Guardando quali e quante organizzazioni gli Anon sono riusciti a violare, però, si può concordare sul fatto che il livello di sicurezza del sistema sanitario nazionale non è precisamente “da manuale”.

L’elenco degli istituti caduti sotto i loro colpi comprende le ASL di Caserta, Rieti e Viterbo, l’ospedale San Giovanni di Roma, ISS, Agenas, Difarma, Federsanità, ASST Lariana e l’ULSS21 di Legnano.

Una vera strage, che dimostra ancora una volta come le varie normative, partendo dal GDPR e passando dalla direttiva NIS (Network and Information Security), stentino a trovare applicazione proprio in quei settori in cui sarebbe più necessario.

I file pubblicati su Internet, a differenza di quanto accaduto in passato in casi simili, non comprendono i dati personali dei pazienti ma soltanto la struttura dei database sottratti. **Insomma: gli hacker si sono limitati a dimostrare di avere la possibilità di accedere a tutti i dati presenti sui server, senza però diffonderli**.

Please follow and like us:

Dalla truffa a luci rosse alla minaccia dell’omicidio su commissione

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/27/anonymous-festeggia-il-natale-violando-i-siti-di-asl-e-ospedali/

Dalla truffa a luci rosse alla minaccia dell’omicidio su commissione

Dic 21, 2018 Marco Schiaffino Attacchi, In evidenza, Minacce, News, Phishing 0

Escalation clamorosa delle truffe via email. Si è passati dal ricatto alla minaccia di piazzare bombe, per arrivare ai sicari assoldati via Internet.

Tutto è cominciato con la cosiddetta "truffa a luci rosse", ma nel giro di poche settimane il gruppo di cyber-criminali che ha lanciato la campagna di email-truffa basate inizialmente su un leak di un sito pornografico ha cominciato a differenziare le sue strategie creando varianti sempre più fantasiose (e improbabili) della truffa originale.

Fino a una decina di giorni fa, le varianti si muovevano sempre sullo stesso tema: l'email prendeva di mira il singolo destinatario (in un primo momento scelto solo tra gli utenti di un sito specifico) e, nella sostanza, si sviluppava sempre con lo stesso canovaccio: **ho hackerato il tuo computer, ti ho spiato (e registrato) mentre guardavi un video porno e ora ti chiedo un riscatto per non diffondere il video a tutti i tuoi contatti**.

Tutto falso, ma la minaccia evidentemente è di quelle che fa una certa presa sull'utente medio e, come abbiamo raccontato ai tempi, ai pirati ha fruttato **un bel po' di soldi**.

Il successo della truffa ha convinto i pirati ad alzare il tiro. Prima hanno cominciato a inviare i messaggi a persone a caso, poi a cambiare il tipo di minaccia.

Nell'ultima settimana si è assistito a un'accelerazione spaventosa. Intorno al 10 dicembre, per esempio, ha fatto la sua comparsa **la "truffa della bomba"**. I pirati, in sostanza, minacciavano di compiere degli attentati dinamitardi se i destinatari dei messaggi non avessero versato **20.000 dollari in Bitcoin** sul loro conto.

A onor del vero, la "truffa della bomba" non ha funzionato un granché. Sui conti dei pirati, infatti, sono arrivati solo

spiccioli e l’unico effetto che avuto è stato quello di creare un certo allarme, concretizzatosi nell’evacuazione di alcuni edifici pubblici (tra ci delle scuole) che erano stati citati nei messaggi minatori.

A seguire, sono comparse altre (e sempre più odiose) varianti, che puntano a fare leva sulle paure delle potenziali vittime attraverso un mix di leggende metropolitane ed episodi di cronaca.

In entrambe le email (ma non è escluso che ne compaiano di nuove e diverse) il mittente si spaccia per l’amministratore di un forum nel Dark Web.

Nella prima, il truffatore sostiene di aver ricevuto la richiesta da parte di una “cliente” che ha chiesto di sfigurare con l’acido (sigh) la vittima della truffa. La logica espressa nel messaggio è semplice: “pagami 1.600 dollari e non subirai l’aggressione”.

L’ultima in ordine di tempo punta ancora più in alto. L’ordine non riguarda più “solo” un’aggressione con l’acido, ma addirittura **un omicidio su commissione**.

In quest’ultima versione, il ragionamento è il seguente: il mio cliente mi paga 4.000 dollari per farti uccidere da un sicario. Se me ne dai 1.600 non solo fermerò il killer, ma ti dirò anche chi è il mandante.

Nelle prossime settimane (ma già nei prossimi giorni) potremo valutare quanto denaro riusciranno a incassare i truffatori e avremo, di conseguenza, un buon parametro per valutare la credulità dell’utente medio.

Please follow and like us:

Bug nei router Huawei: credenziali predefinite e sono tracciabili online

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2018/12/21/dalla-truffa-a-luci-rosse-alla-minaccia-dellomicidio-su-commissione/

La cyber-sicurezza del sistema antimissile USA? Un disastro

Dic 17, 2018 Marco Schiaffino Gestione dati, In evidenza, News, RSS, Scenario, Vulnerabilità 0

Falle di sicurezza, mancati aggiornamenti dei software e scarsi controlli. Per hacker e spie straniere infiltrare i sistemi sarebbe un gioco da ragazzi.

Se vi dicessero che un'azienda non implementa correttamente nessun controllo di sicurezza come autenticazione multi-fattore, verifiche delle vulnerabilità, protezione dei dati

sensibili sulle unità removibili, crittografia delle comunicazioni e protezione dei sistemi fisici di controllo come videocamere e sensori, probabilmente vi si rizzerebbero i capelli in testa.

Difficile immaginare, allora, quale sia la possibile reazione sapendo che questo sconsolante rapporto non riguarda una semplice multinazionale, ma le infrastrutture del **Ballistic Missile Defense System (BMDS)**, cioè il sistema di difesa antimissile degli Stati Uniti d'America.

La stroncatura sulle policy di sicurezza del BMDS arriva direttamente dal **Dipartimento della Difesa**, che ha pubblicato un report (ampiamente censurato prima della pubblicazione) decisamente preoccupante.

La galleria degli orrori, oltre a un generico lassismo nell'introdurre sistemi di sicurezza adeguati a proteggere i sistemi informatici di un'infrastruttura critica, comprende **tempi biblici nell'aggiornamento dei software** (a marzo sono state individuate patch non ancora applicate che avrebbero dovuto essere installate due mesi prima e alcune addirittura risalenti al 2013) e **il mancato utilizzo di crittografia per la protezione dei dati anche quando vengono copiati su unità removibili**.

Le cose non andrebbero meglio anche per quanto riguarda la sicurezza fisica. Stando al rapporto infatti, mancherebbero videocamere di sicurezza in punti in cui ne era prevista l'installazione, non ci sarebbero sistemi di chiusura per i rack dei server e anche il semplice accesso fisico attraverso le porte non sarebbe controllato a sufficienza.

Insomma: un vero disastro, che ha portato gli ispettori a chiedere che **le massime cariche responsabili del BMDS forniscano un commento al rapporto entro l'8 gennaio 2019**. Per gli alti papaveri dell'esercito USA si prospettano quindi delle vacanze di Natale piuttosto impegnative.

Please follow and like us:

Bug nei device Logitech. La falla permetteva di prendere il controllo del PC

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/17/la-cyber-sicurezza-del-sistema-antimissile-usa-un-disastro/

Attacco all’italiana Saipem. PC messi K.O. da una variante di Shamoon

Dic 14, 2018 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware è una versione modificata di quello comparso nel 2012 ed è programmato per cancellare tutti i dati presenti sul disco fisso dei computer.

Prendete una situazione geopolitica complicata come quella del edioriente, aggiungete le tensioni per le fluttuazioni del prezzo del petrolio, completate con un pizzico di strategia e mescolate bene: ecco servito il nuovo capitolo della vicenda **Shamoon**.

Il malware, comparso per la prima volta sui radar delle società di sicurezza 6 anni fa, è un classico caso di cyber-warfare, che vede come protagonisti i paesi del Golfo. Questa volta, però, a farne le spese è stata un’azienda italiana come **Saipem**.

Come riporta un comunicato sul sito ufficiale dell’azienda, l’attacco è avvenuto lo scorso 10 dicembre e ha causato la cancellazione dei dati in alcune infrastrutture IT del gruppo. **L’attacco, nel dettaglio, avrebbe colpito più di 35.000 computer nele sedi in Medioriente, Scozia, India e (in misura minore) Italia**.

Shamoon da un punto di vista tecnico è un **wiper**, cioè un malware programmato per fare piazza pulita di tutti i dati memorizzati sul computer che colpisce. Uno strumento, quindi, non tanto pensato per lo spionaggio, quanto per il sabotaggio.

Il malware era stato utilizzato in passato per colpire **Aramco**, una società petrolifera saudita, e aveva fatto parlare di sé ancora nel 2016, quando una nuova versione del wiper aveva fatto la sua comparsa sempre in Medioriente.

Nel 2017 era comparso invece **Stonedrill**, un malware con caratteristiche molto qualcosa di simili (ne abbiamo parlato in questo articolo) mentre l'ultima azione di sabotaggio su larga scala, anche se con caratteristiche diverse, è stata quella di **NotPetya**, che ha però preso di mira principalmente l'Ucraina.

L'attacco a Saipem, però, sembra inserirsi in quello che potremmo chiamare il "filone originale" di Shamoon. **Prima di tutto perché Saipem, nelle ultime settimane, sembra essere in pole position per aggiudicarsi alcune commesse in collaborazione con Aramco**.

In secondo luogo perché il malware che ha colpito la società italiana è senza dubbio una variante del malware originale comparso nel 2012.

L'analisi degli esperti, sotto questo punto di vista, non lascia dubbi e le conferme arrivano anche da alcuni (strani)

dettagli, come la presenza di **una data di attivazione inserita nel codice del malware, ma che sarebbe impostata per una data (passata) piuttosto lontana: il 7 dicembre 2017 alle ore 23:51**.

Insomma: l'impressione è che qualcuno abbia copiato il codice di un malware pensato per agire come una "bomba a orologeria" e abbia impostato il timer su una data già trascorsa per fare in modo che si attivasse subito.

Please follow and like us:

Truffa da 1 milione di dollari a Save the Children

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/14/attacco-allitaliana-saipem-pc-messi-k-o-da-una-variante-di-shamoon/

Truffa da 1 milione di dollari a Save the Children

Dic 14, 2018 Marco Schiaffino Attacchi, In evidenza, News, RSS 0

Gli hacker hanno violato una casella di posta e hanno inviato all'amministrazione ordini di pagamento per un progetto inesistente.

Ricordate l'immagine romantica dell'hacker in stile Robin Hood che ruba ai ricchi per dare ai poveri? Ecco: scordatevela. Nel terzo millennio l'identikit del pirata informatico è quello di un criminale senza scrupoli, che non guarda in faccia nessuno e non si fa scrupoli nemmeno a colpire un'organizzazione no profit come **Save the Children**.

Come riporta un articolo del **Boston Globe**, l'associazione attiva nel settore della tutela dell'infanzia è stata vittima, nel maggio del 2017, di una classica frode via email, che solo nei primi sei mesi del 2018 secondo l'**FBI** avrebbe fruttato ai cyber-criminali circa 12,5 miliardi di dollari.

Lo schema usato è simile a quello che abbiamo già visto in altre occasioni, anche se questa volta i cyber-criminali hanno messo in piedi una truffa decisamente più complessa.

Tutto è cominciato, stando alla ricostruzione, con **la violazione dell'account di posta elettronica di un dipendente di Save The Children**.

Di solito queste truffe usano tecniche abbastanza semplici, come quella di inviare ordini di pagamento falsi o di modificare l'IBAN di un fornitore per dirottare il pagamento.Gli sciacalli che hanno preso di mira Save the Children invece, hanno fatto qualcosa di molto più complicato.

Una volta avuto accesso all’email dell’impiegato, i pirati informatici hanno creato una serie di documenti e fatture false relative a **un progetto per l’installazione di pannelli solari su alcuni ospedali in Pakistan**, un paese in cui l’associazione è attiva da oltre 30 anni.

Tutto molto credibile, ma anche tutto falso. Il progetto era solo un paravento per giustificare ordini di pagamento per circa **1 milione di dollari** e diretti a un conto corrente che faceva riferimento al **Giappone**. Quando gli impiegati di Save the Children si sono accorti che qualcosa non andava, era troppo tardi. Il denaro era già “evaporato”.

Per fortuna, spiegano fonti dell’associazione, buona parte della somma **è stata coperta da una polizza assicurativa** e la perdita effettiva è stata di “solo” **112.000 dollari**. Il nostro augurio di Natale per i pirati, in ogni caso, è solo uno: che si strozzino con il panettone.

Please follow and like us:

Quanto rischia una nave per un attacco informatico?

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2018/12/14/truffa-da-1-milione-di-dollari-a-save-the-children/

Violati più di 20.000 account di enti del governo italiano

Dic 12, 2018 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, Malware, News, RSS 0

La notizia arriva da Group-IB. Le credenziali di accesso agli account sono in vendita sul Dark Web. Coinvolte in tutto 30 nazioni nel mondo.

È una campagna internazionale, ma ha preso di mira in maniera particolare il nostro paese. Quello descritto da **Group-IB**, in definitiva, potrebbe essere uno dei più clamorosi attacchi rivolti contro enti pubblici e organizzazioni governative.

Il report pubblicato su Internet dalla società di sicurezza

russa parla di **40.000 account violati** che fanno riferimento a siti Internet di **30 nazioni diverse**. A sorprendere è la distribuzione geografica: **il 52%, infatti, sarebbe relativo a utenti italiani**.

Tra i paesi coinvolti ci sono anche Arabia Saudita, Portogallo, Israele, Georgia, Romania, Norvegia e molti altri. Per quanto riguarda il nostro paese, il report di Group-IB fa riferimento al Ministero della Difesa e al Ministero degli Esteri.

Difficile capire se la vicenda riportata dalla società di sicurezza abbia una qualche connessione con la compromissione delle caselle PEC avvenuta lo scorso mese, ma una prima stima basata sui numeri (ai tempi si era parlato di oltre 90.000 account violati) farebbe pensare al contrario.

Quello che è certo è che le credenziali di accesso per il login ai siti **sono attualmente in vendita sul Dark Web** e che il database in questione sembra essere il frutto di una campagna di spionaggio portata avanti per mesi con strumenti diversificati ed estremamente sofisticati.

I ricercatori, infatti, sostengono che le credenziali siano state rubate utilizzando alcuni trojan (come **Azorult**, usato anche nella campagna di truffa a luci rosse) e spyware (**Pony Formgrabber**) che avrebbero consentito ai pirati informatici di

rastrellare le credenziali per l’accesso ai servizi Internet di ministeri e agenzie governative.

Le vittime sarebbero principalmente impiegati pubblici e militari, ma anche “civili” che collaborano con i soggetti compromessi negli ultimi 18 mesi.

Secondo i ricercatori **il database pubblicato nei bassifondi del Web sarebbe ordinato per categorie** (credenziali per servizi bancari, username e password delle caselle di posta, dati per il login dei servizi online) e messi a disposizione di chiunque abbia interesse a comprarli, compresi i **gruppi hacker che lavorano in collaborazione con i servizi segreti di paesi stranieri**.

Please follow and like us:

Trojan per Android ruba soldi da PayPal sotto il naso della vittima

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/12/violati-piu-di-20-000-account-di-enti-del-governo-italiano/

Fatevi un regalo di Natale: disinstallate Flash!

Dic 10, 2018 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Il suggerimento arriva da G Data, dopo la notizia dell'ennesimo exploit zero-day che sfrutta le falle del programma Adobe.

Un po' sopra le righe, ma condivisibile. Il commento di **Hauke Gierow** di **G Data** sull'ennesima vulnerabilità di **Adobe Flash** è perentoria: "Suggerimento di sicurezza per queste vacanze: disinstallare Flash".

A suscitare l'ironico commento del ricercatore è una falla di sicurezza (CVE-2018-15982) che non colpisce direttamente le applicazioni Flash, ma i documenti in formato **DOC** attraverso i plugin **Active X**.

E anche se Adobe ha pubblicato con tempestività un aggiornamento per correggere la falla, dalle parti di Bochum (sede della società di sicurezza tedesca) devono averla considerata come la classica goccia che fa traboccare il vaso.

Tanto più che, in questo caso, la vulnerabilità non è stata individuata da un ricercatore di sicurezza a caccia di bug nel software Adobe, ma **è emersa dopo che è stata sfruttata per portare attacchi informatici di alto livello**.

A utilizzarla è stata nientemeno che la famigerata **Hacking Team**, la società milanese specializzata in software spia che vende a forze di polizia e servizi segreti di tutto il mondo, finita al centro delle polemiche già nel 2015 quando **WikiLeaks** pubblicò migliaia di email interne rubate da un misterioso hacker in cui emergevano comportamenti poco "attenti ai diritti umani" nella scelta dei clienti.

Un'accusa che Hacking Team si trova a fronteggiare anche in questi giorni, dopo che il **Washington Post** ha pubblicato un articolo in cui sostiene che la società lombarda abbia fornito strumenti di spionaggio ai responsabili dell'atroce assassinio del giornalista **Jamal Khashoggi**.

Tornando a Flash, il post pubblicato da G Data sottolinea come le vulnerabilità legate al software siano estremamente frequenti e sistematicamente sfruttate dai cyber-criminali per portare attacchi.

E se le alternative esistono (**HTML 5** è il candidato naturale a sostituirlo) non mancano gli elementi di preoccupazione. **A partire dal 2020, infatti, Adobe non fornirà più il supporto per la sua tecnologia**.

Tradotto: a nuove falle non corrisponderanno nuovi

aggiornamenti. Se il mondo dell’Information Technology non avrà fatto definitivamente pizza pulita di tutto ciò che rimanda a Flash per allora, rischiamo di vederne delle belle.

Please follow and like us:

In Australia una legge contro la crittografia. Arrivano le backdoor di stato?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/10/fatevi-un-regalo-di-natale-disinstallate-flash/

Il Privileged Access Management è un priorità anche per Gartner

Dic 07, 2018 Marco Schiaffino In evidenza, Mercato, News, Scenario, Tecnologia 0

Anche Gartner, finalmente, sancisce l'importanza di questo aspetto della sicurezza pubblicando il suo primo "Magic Quadrant" a proposito.

Chi si occupa di sicurezza probabilmente aveva le idee chiare sull'importanza del **Privileged Access Management (PAM)** anche senza bisogno di ulteriori conferme, ma l'endorsement di un soggetto come **Gartner** rappresenta di certo un segnale che per il settore non passa inosservato.

La società, infatti, ha pubblicato il primo Magic Quadrant dedicato al PAM, accompagnandolo con una dichiarazione che lascia pochi dubbi: *"La gestione degli accessi privilegiati è uno dei controlli di sicurezza più critici, in particolare nell'attuale ambiente IT sempre più complesso. I leader della sicurezza e della gestione dei rischi devono utilizzare gli strumenti PAM in una strategia a lungo termine per una completa attenuazione dei rischi."*

La gestione degli accessi, in quest'ottica, non rappresenta più un settore di nicchia ma una vera e propria priorità, soprattutto per le istituzioni finanziarie, gli enti pubblici e il settore medicale.

La conferma di questa prospettiva arriva dalla cronaca di tutti i giorni, che mostra come i cyber-criminali puntino sempre più spesso a prendere di mira le credenziali di impiegati e manager per ottenere l'accesso a dati riservati e segreti industriali.

Secondo **CyberArk**, inserita come leader nel Magic Quadrant di Gartner dedicato al Privileged Access Management, **il 100% degli attacchi avanzati sfrutta credenziali privilegiate** e il 70% degli attacchi portati da soggetti collegati a governi stranieri utilizza il phishing (e conseguentemente la violazione di credenziali – ndr) come vettore iniziale.

Non stupisce, quindi, che la stessa Gartner preveda una crescita esponenziale nella diffusione di queste tecnologie, che nel 2021 dovrebbero essere integrate dal **40% delle organizzazioni** (nel 2018 la penetrazione è stimata al 10%) all'interno dei loro sistemi di sicurezza.

Una reazione che potremmo definire "normale", soprattutto a fronte del fatto che, secondo indagini di mercato, **il 72% delle organizzazioni non si sentirebbe al sicuro per quanto riguarda i sistemi di controllo per l'accesso da parte degli impiegati alle informazioni sensibili**.

Potete scaricare il rapporto Magic Quadrant 2018 di Gartner per il Privileged Access Management direttamente dal sito di CyberArk, cliccando qui.

Please follow and like us:

DarkVishnya: attacchi alle banche come nei film di Hollywood È cinese il pirata informatico più scarso della storia

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2018/12/07/il-privileged-access-management-e-una-priorita-di-sicurezza/

È cinese il pirata informatico più scarso della storia

Dic 07, 2018 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Ha fatto più di 100.000 vittime in pochi giorni con un ransomware, ma ha lasciato dietro di sé una montagna di indizi. Tracciato e arrestato in 4 giorni.

Quando lo scorso 1 dicembre ha diffuso il suo ransomware **UNNAMED1989**, il 22enne **Luo Moumou** deve aver pensato di essere riuscito a mettere a segno un vero colpaccio.

Il suo malware, infatti, si è diffuso con una velocità sorprendente e ha colpito più di 100.000 computer nel giro di soli 3 giorni.

Per diffonderlo, Moumou ha utilizzato una cinquantina di app, tra cui una utilizzata per gestire più account di QQ, un programma di messaggistica popolarissimo in Cina.

UNNAMED1989, stando a quanto riportano i ricercatori di **Tencent**, è un malware tutt'altro che complesso ed è progettato per eseguire due compiti principali: rubare gli account di alcuni servizi online e avviare un modulo ransomware che **crittografa tutti i dati presenti sul PC e chiede un (modesto) riscatto di 110 Yuan, circa 16 dollari**.

Il ransomware visualizza la classica richiesta di riscatto fissando un termine perentorio per il pagamento, passato il quale cancellerebbe la chiave. La crittografia dei dati, però, viene effettuata con XOR, un algoritmo di cifratura decisamente debole che i ricercatori hanno scardinato facilmente.

Ma l'uso di un algoritmo poco affidabile è stato l'errore meno grave fatto da Moumou. L'apprendista pirata, infatti, ha anche scelto **WeChat** come strumento di pagamento per il riscatto. Un'idea decisamente poco brillante, che già da sola avrebbe aperto alla possibilità di rintracciarlo.

Tanto per non correre il rischio di farla franca, Moumou ha anche lasciato altre tracce che i ricercatori hanno individuato analizzando il codice del ransomware. **Da qui sono riusciti a recuperare un nome, un numero di cellulare, un indirizzo email e un account QQ**.

IL 22enne è stato arrestato il 5 dicembre e ha confessato di essere l'autore e il responsabile della diffusione di UNNAMED1989, segnando così la fine della più breve carriera nella storia del cyber-crimine.

Please follow and like us:

Voragine di sicurezza in Kubernetes. A rischio i sistemi cloud

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2018/12/07/e-cinese-il-pirata-informatico-piu-scarso-della-storia/