Tsunami: il software di sicurezza targato Google diventa open

Lug 10, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

Il colosso statunitense ha deciso di rilasciare liberamente la sua piattaforma pensata per l'analisi e l'individuazione delle falle di sicurezza.

Per gli appassionati della filosofia **open source**, la sicurezza informatica è una sorta di isola felice. Non solo perché la collaborazione tra società di sicurezza e lo scambio di informazioni è una pratica ormai sedimentata da tempo, ma anche perché tutte le società tecnologiche sono ormai convinte che una rete sicura è un vantaggio per tutti.

L'ennesima conferma arriva da **Google**, che ha annunciato nelle scorse ore di voler mettere a disposizione di chiunque lo voglia il suo software **Tsunami**. Il tutto in una prospettiva squisitamente open source.

Tsunami è un programma pensato per gestire grandi infrastrutture e fare ciò che per un tecnico sarebbe impossibile fare manualmente quando si ha a che fare con centinaia di migliaia di server: analizzarne le impostazioni per individuare eventuali punti deboli.

Il software, in particolare, è in grado di rilevare eventuali problemi in ambienti estremamente complessi, in cui oltre alle tradizionali workstation ci sono anche apparati di rete e dispositivi IoT. **Insomma, nonostante il nome, Tsunami è pensato per mettere ordine dove normalmente regna il caos**.

A differenza di altri strumenti simili, riesce infatti a compiere un’unica scansione su dispositivi di tipo diverso, riducendo notevolmente il livello di complessità di questo tipo di operazioni.

Una volta mappata la rete, il programma analizza le porte esposte di ogni dispositivo ed esegue dei test per verificare se siano vulnerabili ad attacchi conosciuti. In particolare, Tsunami si concentra sui servizi raggiungibili dall’esterno e che non sono protetti da sistemi di autenticazione o utilizzano credenziali deboli.

Insomma, il tema è quello dei rischi legati ad attacchi che sfruttano impostazioni inadeguate, qualcosa che da queste pagine ci è toccato raccontare (troppo) spesso.

Naturalmente a essere interessate a uno strumento del genere sono le aziende di grandi dimensioni (e per “grandi” si intende allo stesso livello di Google) e questo spiega anche la decisione dell’azienda statunitense di rendere il progetto il più “neutro” possibile.

Oltre a essere open source, Tsunami non verrà etichettato come un prodotto Google ma sarà destinato a diventare una sorta di

“bene comune” a disposizione di tutti.

Condividi l’articolo

Sul Dark Web sono in vendita 15 miliardi di credenziali rubate

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/10/tsunami-il-software-di-sicurezza-targato-google-diventa-open/?utm_source=rss&utm_medium=rss&utm_campaign=tsunami-il-software-di-sicurezza-targato-google-diventa-open

---

Sul Dark Web sono in vendita 15 miliardi di credenziali rubate

Lug 09, 2020 Marco Schiaffino Gestione dati, Hacking, In evidenza, News, RSS, Scenario 0

Il numero di username e password sottratti è aumentato del 300% rispetto al 2018. Sul mercato nero valgono un vero capitale.

Il settore delle credenziali rubate non conosce crisi. Anzi:

si tratta di un business che è in piena crescita. A confermarlo è un report pubblicato dal **Digital Shadows Photon Research Team**, in cui viene analizzato il fenomeno fornendo dati che fanno accapponare la pelle.

Il primo riguarda il numero di credenziali in vendita sul Dark Web, che ha raggiungo la cifra di **15 miliardi**, in pratica 2 per ogni abitante del pianeta terra. Di queste, 5 miliardi sono "uniche".

Gli autori del report spiegano che la maggior parte delle credenziali che i pirati informatici commerciano nei bassifondi di Internet sono relative a utenti privati, molte delle quali vengono semplicemente fornite gratis.

Nel caso in cui sia richiesto un pagamento, il prezzo (la media è di 15 dollari) varia a seconda della tipologia di servizio. **I più costosi sono quelli relativi ai servizi di home banking, che sono valutati intorno ai 70 dollari**. I ricercatori specificano che questo tipo di credenziali rappresentano il 25% di quelle "pubblicizzate" per la vendita.

Le cifre salgono quando si parla di credenziali che consentono l'accesso ai sistemi di organizzazioni e aziende, con un

prezzo medio di 3.139 dollari e una punta massima, registrata in un’asta, di 140.000 dollari.

Ma da dove arrivano tutte queste credenziali rubate? L’analisi non contiene grosse sorprese: le fonti sono attacchi con malware, azioni di phishing e iniezioni di codice malevolo all’interno delle pagine Web che ospitano i moduli di login.

L’interno report offre un panorama piuttosto variegato, in cui spicca la disponibilità di strumenti dedicati al furto di account. Limitandosi al settore del **credential stuffing** (l’uso di credenziali rubate per tentare il login in altri servizi – ndr) il rapporto cita sei diversi software specializzati in questo tipo di attività.

L’elemento più preoccupante, però, è che secondo i ricercatori i sistemi di autenticazione multi-fattore non rappresentano un ostacolo insormontabile per il furto di account. **I pirati informatici, infatti, sarebbero in grado di aggirarne numerose tipologie, a partire ovviamente da quelli basati su OTP via SMS**.

Condividi l’articolo

Tsunami: il software di sicurezza targato Google diventa open
Mozilla sospende Firefox Send: “usato per distribuire malware”

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/09/sul-dark-web-sono-in-vendita-15-miliardi-di-credenziali-rubate/?utm_source=rss&utm_medium=rss&utm_campaign=sul-dark-web-sono-in-vendita-15-miliardi-di-credenziali-rubate

Mozilla sospende Firefox Send: “usato per distribuire malware”

Lug 08, 2020 Marco Schiaffino Attacchi, Gestione dati, In evidenza, Malware, News, Prodotto, RSS, Scenario 0

Il servizio per l’invio e la condivisione di file veniva utilizzato dai pirati informatici per distribuire trojan, ransomware e altri malware.

Anche i migliori possono inciampare in qualche errore. **Firefox**

Send, il sistema di condivisione dei file gestito da **Mozilla**, è finito nell'occhio del ciclone per essere diventato uno strumento utilizzato intensivamente da gang di cyber criminali. Per il momento il servizio è stato sospeso, ma è difficile capire se e quando potrà essere di nuovo disponibile.

Il sistema, lanciato nel 2019, consentiva di caricare sui server di Mozilla i file e distribuirli attraverso un link per il download. Il servizio utilizzava un sistema di crittografia e consentiva di prevedere l'uso di una password per accedervi e impostare un numero massimo di download possibili.

Una serie di funzionalità decisamente utili, ma molto appetibili anche per i pirati informatici. Numerosi esperti di sicurezza hanno infatti segnalato come Firefox Send sia stato utilizzato per distribuire malware sfruttando proprio le caratteristiche del servizio.

[embedded content]

Tra i gruppi di cyber criminali che avrebbero sfruttato il servizio ci sarebbe anche **Revil**, la gang che distribuisce il ransomware **Sodinokibi** e che ha fatto parlare molto di sé negli ultimi mesi.

A ben vedere, le funzioni messe a disposizione da Mozilla sono ideali per questo scopo. La crittografia, così come la protezione con password, permettono di impedire la scansione dei file da parte di buona parte dei software antivirus.

Senza contare che i link che fanno riferimento ai server di Mozilla vengono automaticamente considerati legittimi dai filtri basati su liste di esclusione.

Anche la possibilità di impostare un numero massimo di download, raggiunto il quale i file vengono cancellati, rappresenta un ottimo strumento per cancellare le tracce dell'attacco.

La decisione di chiudere temporaneamente il servizio è arrivata dopo che un gruppo di ricercatori ha inviato un report riguardante l'abuso del servizio, in cui si chiedeva a Mozilla di inserire una funzione che consentisse di segnalare utilizzi impropri di Firefox Send.

L'azienda, però, ha deciso di agire in maniera più drastica e ha bloccato tutto, avviando probabilmente una revisione delle modalità di funzionamento per impedire che in futuro si ripetano casi come quelli denunciati.

Condividi l'articolo

Allarme dei servizi segreti USA: i pirati prendono di mira gli MSP

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/08/mozilla-sospende-firefox-send-usato-per-distribuire-malware/?utm_source=rss&utm_medium=rss&utm_campaign=mozilla-sospende-firefox-send-usato-per-distribuire-malware

---

Allarme dei servizi segreti USA: i pirati prendono di

mira gli MSP

Lug 07, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Gli attacchi nei confronti dei Managed Service Provider consentono ai cyber criminali di colpire a cascata tutti i sistemi che gestiscono.

Sempre più sfacciati e disposti a correre rischi per colpire il "bersaglio grosso" e massimizzare danni (e profitti) dei loro attacchi. È questo l'identikit dei cyber criminali che, secondo i servizi segreti USA, stanno sistematicamente prendendo di mira i **Managed Service Provider (MSP)** con i loro attacchi.

Come si legge nel report pubblicato da **ZDNet** a questo indirizzo Internet, il modus operandi dei pirati informatici prevede la compromissione dei sistemi informatici degli MSP con lo scopo di infiltrare le aziende che fruiscono dei loro servizi.

Una strategia che consente ai cyber criminali di ottenere un accesso privilegiato ai sistemi delle potenziali vittime e sfruttarlo per portare attacchi di ogni genere. Il documento del **Global Investigative Operations Center (GIOC)** elenca le attività rilevate.

Queste comprendono le ormai classiche truffe BEC (Business Email Compromise) e intrusioni nei sistemi di pagamento elettronici POS. **Il report, però, segnala come il rischio maggiore sia rappresentato dalla possibilità che gli accessi ai servizi vengano utilizzati per attacchi ransomware**.

L'allarme, sottolineano gli esperti di sicurezza, focalizza l'attenzione su un fenomeno cresciuto esponenzialmente nel corso del 2019, in cui la cronaca ha registrato attacchi a decine di Managed Service Provider.

Analizzando le raccomandazioni che il GIOC, nel suo documento, indirizza alle aziende che usufruiscono dei servizi gestiti, appare chiaro come la principale preoccupazione sia quella legata alla gestione dei **sistemi di controllo remoto (RDP)**, che più di altri servizi consentono un facile accesso ai cyber criminali.

Per quanto riguarda gli MSP, le raccomandazioni sono quelle cui dovrebbero attenersi tutte le aziende e gli operatori in

ambito di cyber security: aggiornamento dei sistemi, adeguamento agli standard legali e, soprattutto, formazione continua dei dipendenti per metterli al riparo dagli attacchi.

IL dato che emerge, però, è che questa nuova declinazione degli attacchi supply chain sta assumendo dimensioni tali da allertare addirittura i servizi segreti.

Condividi l’articolo

Hackerano siti di news per colpire decine di aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/07/allarme-dei-servizi-segreti-usa-i-pirati-prendono-di-mira-gli-managed-service-provider/?utm_source=rss&utm_medium=rss&utm_campaign=allarme-dei-servizi-segreti-usa-i-pirati-prendono-di-mira-gli-managed-service-provider

---

Hackerano siti di news per colpire decine di aziende

Lug 06, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il gruppo Evil Corp ha usato una strategia in due fasi per introdursi nelle reti aziendali e installare il ransomware WastedLocker.

In un primo momento era sembrato un “normale” attacco di massa nei confronti di decine di imprese statunitensi. In seguito, però, i ricercatori di **Symantec** hanno scoperto che i tentativi di violazione subiti dalle aziende seguivano una strategia decisamente elaborata.

Come si legge nel report pubblicato dalla società di sicurezza, infatti, **gli autori degli attacchi hanno usato come “trampolino di lancio” una dozzina di siti di news che avevano compromesso in precedenza**.

Protagonista di questa vicenda è il gruppo **Evil Corp**, conosciuto per aver diffuso in passato il malware **Dridex**. Stando alla ricostruzione di Symantec, la gang di cyber criminali avrebbe preso di mira un gruppo editoriale statunitense, ottenendo l’accesso ai server che ospitano 12 siti di news.

I pirati hanno sfruttato questa opportunità iniettando sulle pagine dei siti il codice di **SocGholish**, un malware basato su piattaforma JavaScript che ha permesso loro di colpire i dipendenti delle aziende che visitavano le pagine infette.

I bersagli, tutti con sede negli USA, operano in settori molto diversificati e la loro scelta appare essere dettata più che altro dalla possibilità di massimizzare il profitto derivante dagli attacchi.

La tecnica utilizzata è stata quella di visualizzare delle false richieste di aggiornamento software, che avviavano il download e l'installazione di **Cobalt Strike**, uno strumento di hacking che consente di eseguire comandi sul computer compromesso, avviare ulteriori processi e caricare e scaricare file.

Da qui, i pirati di Evil Corp hanno cercato di avviare una serie di attività nella logica del "movimento laterale", con l'obiettivo di individuare le infrastrutture critiche delle aziende e installare il ransomware **WastedLocker**.

L'attacco, come spiegano gli autori del report, è stato sventato. La vicenda, però, rappresenta l'ennesima dimostrazione del fatto che i gruppi di cyber criminali utilizzano strategie sempre più complesse, senza farsi scrupoli degli "effetti collaterali" legati ai loro attacchi.

Condividi l'articolo

La polizia hackera Encrochat per incastrare i criminali

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/06/evil-corp-hackerano-siti-di-news-per-colpire-decine-di-aziende/?utm_source=rss&utm_medium=rss&utm_campaign=evil-corp-hackerano-siti-di-news-per-colpire-decine-di-aziende

La polizia hackera Encrochat per incastrare i criminali

Lug 03, 2020 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario 0

Le polizie europee sono riuscite a scardinare il sistema di "comunicazioni sicure". I messaggi intercettati hanno portato a decine di arresti e sequestri.

Una clamorosa operazione di hacking ha permesso alle forze di polizia di Francia, Olanda e Regno Unito di smantellare un numero impressionante di organizzazioni criminali. L'azione, gestita dall'unità di cooperazione **EuroJust**, ha preso di mira un'azienda specializzata nella fornitura di telefoni "sicuri" molti utilizzati dalla malavita per proteggere le loro comunicazioni.

La società al centro della vicenda è Encrochat, impresa che

opera alla luce del sole (almeno da un punto di vista formale) e fornisce “soluzioni di sicurezza end to end” orientate a “garantire l’anonimato”.

Come si legge nell’inchiesta pubblicata da **Vice**, i dispositivi messi a disposizione di Encrochat sono versioni “modificate” di normali terminali Android, sui quali vengono eseguiti interventi fisici per impedire il funzionamento di GPS e fotocamera.

Gli smartphone, inoltre, permettono di utilizzare due sistemi operativi che “convivono” sul dispositivo e che l’utilizzatore può selezionare a suo piacimento. La logica è quella di poter utilizzare un sistema che non genera alcun sospetto agli occhi di un eventuale osservatore e poter accedere a quello “blindato” solo quando serve.

I telefoni integrano anche un sistema di emergenza che consente al proprietario di cancellarne tutto il contenuto semplicemente inserendo un PIN specifico.

Encrochat, però, non si limita a fornire i dispositivi: fornisce anche il software di crittografia che permette di codificare le chiamate e i messaggi, gestendo anche il server centralizzato che ne consente lo scambio. Il costo del servizio che comprende l’u

Il sistema avrebbe consentito ai criminali di gestire i loro traffici con la massima tranquillità, senza doversi preoccupare del rischio di eventuali intercettazioni.

L’operazione di EuroJust, però, ha fatto saltare il sistema. Anche se non vengono forniti dettagli sulle modalità utilizzate, gli agenti sono infatti riusciti a violare le protezioni e accedere a tutti i messaggi e le conversazioni trasmessi sul circuito Encrochat.

A partire dallo scorso aprile, il gruppo di investigatori ha potuto analizzare milioni di comunicazioni, scoprendo che i criminali utilizzavano il sistema di messaggistica e di telefonia senza adottare alcuna ulteriore precauzione, fornendo dettagli su crimini violenti, pianificazioni di omicidi e attività connesse al traffico di droga all’ingrosso.

I risultati sono riassunti nel comunicato stampa ufficiale di EuroJust: nella sola Olanda, l’operazione avrebbe portato all’arresto di 60 sospetti, il sequestro di ingenti quantità di droga (10 tonnellate di cocaina; 70 chili di eroina; 12 tonnellate di cannabis e 1,5 tonnellate di metanfetamina) e lo

smantellamento di 19 laboratori per la sintesi di droghe.

I sequestri avrebbero interessato anche armi automatiche, 25 veicoli utilizzati per il contrabbando di droga e circa 20 milioni di euro in contanti.

Le operazioni della polizia europea hanno però allertato gli operatori, che l scorso 13 giugno hanno realizzato cheil servizio era ormai compromesso e hanno interrotto ogni attività.

Condividi l’articolo

Hackera 23.000 server MongoDB e chiede il riscatto “ai sensi del GDPR”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/03/hackerato-encrochat-il-network-telefonico-crittografato-della-malavita/?utm_source=rss&utm_medium=rss&utm_campaign=hackerato-encrochat-il-network-telefonico-crittografato-della-malavita

---

Hackera 23.000 server MongoDB e chiede il riscatto “ai

sensi del GDPR”

Lug 02, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, News, RSS, Scenario 0

Il pirata informatico chiede 120 euro per non denunciare gli amministratori dei server alle autorità di garanzia della privacy.

Chi pensava che la corretta applicazione del **GDPR** non sarebbe stata supportata da controlli adeguati, oggi deve ricredersi. L’unico elemento inaspettato è che la sorveglianza sul rispetto delle norme sulla protezione dei dati non viene esercitata dalle autorità europee, ma dai pirati informatici.

Si tratta, in realtà, di una variante degli attacchi ransomware visti già qualche tempo fa e che prendono di mira gli amministratori IT troppo distratti (o pigri) per ricordarsi di proteggere l’accesso ai loro database con username e password.

Se in passato, però, i pirati informatici cancellavano i dati minacciando di non restituirli in caso di mancato pagamento del riscatto, oggi hanno trovato un altro strumento di pressione per le loro cyber-estorsioni: **minacciare l’amministratore di denunciare il mancato rispetto delle norme GDPR**.

Il fenomeno non è nuovo ma l’ultimo caso, segnalato dal **Victor Gevers**, ha davvero del clamoroso. Il ricercatore ha infatti segnalato sui social network una campagna di estorsioni apparentemente condotta da un singolo hacker, che avrebbe colpito la bellezza di 23.000 server **MongoDB**.

Il modus operandi del cyber criminale è piuttosto semplice: utilizza degli strumenti automatizzati per individuare i

server esposti su Internet senza credenziali di accesso, copia i dati memorizzati al loro interno e poi lascia una richiesta di "riscatto" in cui **minaccia esplicitamente di denunciare alle autorità l'assenza di precauzione adeguate nella conservazione dei dati**.

La strategia adottata dallo sconosciuto hacker, in ogni caso, è piuttosto brillante. Considerato il fatto che una violazione del GDPR può portare a multe piuttosto salate (fino al 4% del fatturato annuo dell'azienda) una richiesta di riscatto di soli 0,015 Bitcoin (123 euro al cambio attuale) può essere facilmente accettata da qualsiasi azienda che non voglia correre il rischio di subire indagini o sanzioni.

D'altra parte anche una somma modesta come quella richiesta, se pagata da una buona percentuale dei 2**3.000 server compromessi**, si trasforma in un bel tesoretto. Soprattutto se si considera il fatto che il pirata informatico in questione non si è certo ammazzato di lavoro.

Tutto quello che ha fatto, in fondo, è stato mettere a punto un sistema automatizzato per individuare i server configurati in maniera insicura.

Condividi l'articolo

La crittografia è diventata una priorità

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/02/hackera-23-000-server-mongodb-e-chiede-il-riscatto-ai-sensi-del-gdpr/?utm_source=rss&utm_medium=rss&utm_campaign=hackera-23-000-server-mongodb-e-chiede-il-riscatto-ai-sensi-del-gdpr

La crittografia è diventata una priorità

Lug 01, 2020 Marco Schiaffino Approfondimenti, In evidenza, Scenario, Tecnologia 0

Lo dice il Thales Data Threat Report 2020. Le aziende stanno finalmente prendendo sul serio la protezione dei dati?

Quando si parla di report e statistiche nella cyber security, di solito c'è poco da stare allegri. In questo caso, però, i dati che emergono dal **Thales Data Threat Report 2020** suonano quasi rassicuranti.

L'indagine presentata oggi dall'azienda francese concentra la sua attenzione sulla protezione dei dati e raccoglie i

risultati delle interviste a 509 organizzazioni, sia pubbliche che private, con sede in Europa.

Lo scenario di partenza, giocoforza incentrato sull'incidenza dei data breach, dimostra l'attualità della tematica legata alla cyber security, con **il 28% degli intervistati che ha ammesso di aver subito violazioni nell'ultimo anno**.

E se le statistiche relative allo storico non sono certo entusiasmanti, come confermano i dati relativi al fatto che il 95% dei dati rubati non fossero cifrati o la stima di un 69% degli incidenti originati da furti di credenziali o dall'uso di credenziali deboli, lo scenario che emerge per il prossimo futuro è decisamente più roseo.

Il ragionamento parte da quel fenomeno di trasformazione digitale che sta portando le aziende a considerare più seriamente (complici anche le nuove normative e il solito GDPR) il tema della protezione dei dati.

“Le piattaforme cloud e l’uso di servizi decentrati rende impensabile adottare una strategia di difesa del perimetro come quella tradizionale” spiega **Luca Calindri** di Thales. “In questo nuovo contesto l’obiettivo a livello di sicurezza è quello di neutralizzare il danno attraverso la protezione dei dati e dell’identità digitale”.

Una spinta verso la sicurezza

Dando per assunto questo rapporto tra adozione di piattaforme cloud e presa di coscienza del tema della protezione del dato, le statistiche sull’adozione delle piattaforme cloud a livello europeo lasciano ben sperare.

Dal rapporto, infatti, emerge come il 46% di tutti i dati delle organizzazioni sia archiviato nel cloud e ben il 43% di questi dati sia considerato “sensibile” e di conseguenza emerga la necessità (finalmente percepita dalle aziende) di proteggerlo in maniera efficace.

“L’Italia ha un tasso di adozione leggermente inferiore, ma c’è una forte accelerazione nel nostro paese relativo sia all’adozione di nuove tecnologie, sia dalla sempre maggiore importanza della cyber security” puntualizza Calindri.

Tutto bene, quindi? Non ancora. Prima di tutto perché, stando ai dati raccolti da Thales, per il momento solo il 54% dei dati sensibili è protetto da crittografia. In secondo luogo perché nel settore si sconta ancora un certo livello di confusione.

Se si guarda alle modalità di implementazione del cloud, infatti, si scopre che l’80% delle aziende utilizza almeno due piattaforme contemporaneamente. Una situazione che aumenta il livello di complessità.

Uno dei temi più spinosi, in questo ambito, è inoltre il fatto che molte aziende non interiorizzano il fatto che la sicurezza del dato è responsabilità dell’azienda e non del fornitore di servizi cloud. Si apre, insomma, una sorta di “area grigia” in cui il problema della cyber security non viene sempre affrontata in maniera adeguata.

Per quanto riguarda il tema della gestione della cifratura dei dati, per esempio, le imprese tendono ad adottare le soluzioni più “semplici”, in cui la gestione della crittografia come quella delle chiavi è affidata al provider di servizi cloud.

Meno frequente la scelta di soluzioni secondo la formula “**Bring Your Own Key**” o “**Hold Your Own Key**”, in cui la gestione è spostata verso l’utente e offre una maggiore garanzia di sicurezza. Ancora meno diffusa la formula “**Bring Your Own Encryption**”, che affida ogni aspetto di gestione direttamente all’azienda, consentendo di centralizzare completamente le funzionalità di cifratura.

Le sfide del futuro prossimo

Uno degli elementi che emergono in questa “corsa alla

protezione dei dati” è anche la preoccupazione per gli scenari prossimi venturi e in particolare per la possibilità che il settore della crittografia per come la conosciamo subisca uno scossone dall’avvento del Quantum Computing.

“Chi opera nel settore ha già messo in conto che questo cambiamento ci obbligherà ad adattarci” conferma Calindri. “Gli algoritmi che oggi consideriamo sicuri, potrebbero diventare insufficienti a garantire una protezione efficace nell’arco di 5 o 10 anni”.

Un orizzonte piuttosto vicino, che Thales sta affrontando attraverso l’avvio di progetti con partner esterni che puntano a elaborare sistemi di crittografia “irrobustiti” attraverso un generatore di entropia esterno.

L’ipotesi che i computer quantistici possano portare a una modifica nelle logiche stesse adottate per la creazione degli

algoritmi, anche se non viene scartata a priori, rimane invece per il momento sullo sfondo. Il motivo è semplice e ha fondamenti estremamente pratici che affondano nella necessità di rispettare gli standard stabiliti a livello internazionale.

In altre parole, alla luce di una normativa che diventa sempre più “reattiva” rispetto alle nuove esigenze, qualsiasi soggetto coinvolto nel settore deve entrare nell’ottica di seguire la linea comune.

Condividi l’articolo

Come si è evoluta la threat intelligence e quale direzione prenderà nel 2020

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/01/la-crittografia-e-diventata-una-priorita/?utm_source=rss&utm_medium=rss&utm_campaign=la-crittografia-e-diventata-una-priorita

---

Tutti i rischi di sicurezza delle infrastrutture

pubbliche

Giu 30, 2020 Marco Schiaffino Hacking, In evidenza, Leaks, News, Privacy, RSS, Scenario, Tecnologia 0

La digitalizzazione dei servizi pubblici e governativi consente un miglioramento a livello di efficienza, ma sono protette in maniera adeguata?

Quando si parla di informatica e strumenti digitali, il termine "aperto" suscita immediata simpatia. Che si tratti di codici sorgenti o database, l'idea che le informazioni siano accessibili a tutti ci rassicura. Esiste però un rovescio della medaglia, rappresentato dai rischi di sicurezza.

A spiegarlo in un intervento pubblicato su **Bleeping Computer** è il ricercatore **Ax Sharma**, che mette sotto la lente d'ingrandimento tutti gli usi "distorti" che potrebbero essere fatti di queste informazioni da parte di soggetti malintenzionati, come un governo ostile.

Il suo ragionamento parte da un report che ha pubblicato un paio di settimane fa riguardo l'esposizione dei dati di un database utilizzato per il riconoscimento automatico delle targhe tramite videocamere nel Regno Unito.

Nel corso dello studio, Sharma ha infatti scoperto che molte delle videocamere in questione sono liberamente accessibili a chiunque. **Non si tratta di un errore di configurazione, ma di una scelta dettata dalla legislazione britannica in tema di trasparenza**.

La domanda che il ricercatore si pone riguarda la possibilità che informazioni del genere (si tratta di videocamere per il monitoraggio del traffico) possano essere utilizzate per provocare danni alla collettività. La risposta, purtroppo, è affermativa.

Informazioni del genere per esempio, potrebbero essere utilizzate per massimizzare i danni di un attacco terroristico o un sabotaggio ai danni dei sistemi che gestiscono il traffico.

Anche quando non si parla di dati "aperti", rimane il problema della percezione del rischio e del livello di protezione che viene garantito ai dati. Se le cosiddette "infrastrutture critiche" (come centrali elettriche, impianti nucleari e simili) possono godere di particolari protezioni, lo stesso non si può dire di infrastrutture altrettanto sensibili ma la cui importanza è meno evidente, per lo meno agli occhi dell'opinione pubblica.

Uno degli esempi portati da Sharma è quello dei servizi di emergenza sanitaria, che negli ultimi mesi sono finiti sotto

stress a causa della pandemia da **Covid-19**. Un attacco in grado di mandare in tilt i sistemi in un periodo del genere, sottolinea il ricercatore, avrebbe conseguenze catastrofiche.

Insomma: la declinazione “pubblica” della trasformazione digitale ha in sé aspetti terribilmente delicati e contemperare trasparenza, libertà di accesso e sicurezza non è certamente facile. Un tema, questo, su cui le pubbliche amministrazioni dovrebbero probabilmente avviare una (seria) riflessione.

Condividi l’articolo

In Australia il governo lancia l’allarme: “Siamo sotto attacco”

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/30/tutti-i-rischi-di-sicurezza-delle-infrastrutture-pubbliche/?utm_source=rss&utm_medium=rss&utm_campaign=tutti-i-rischi-di-sicurezza-delle-infrastrutture-pubbliche

---

In Australia il governo lancia l’allarme: “Siamo

sotto attacco”

Giu 29, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS 0

Il comunicato delle istituzioni australiane denuncia un’attività estremamente sofisticata da parte di hacker legati a un governo straniero. È la Cina?

Un vero bombardamento di attacchi hacker ai danni di siti, enti pubblici e organizzazioni su territorio australiano. A descriverlo è un corposo report dell’**Australian Cyber Security Centre (ACSC)** in cui vengono descritti nei dettagli gli strumenti e le tecniche di attacco utilizzate dai pirati.

Quella descritta dagli analisti australiani è una campagna di hacking di proporzioni enormi, che sfrutta diverse tecniche di attacco e che, secondo le dichiarazioni di alcuni esponenti governativi, potrebbe essere legata all’attività del governo cinese.

Sotto un profilo tecnico, gli attacchi variano dall’utilizzo di exploit noti all’uso di tecniche di spear phishing dirette a dirigenti e impiegati pubblici. In particolare, sottolineano i ricercatori dell’ACSC, i pirati starebbero cercando di sfruttare alcune vulnerabilità (CVE-2019-18935, CVE-2017-9248, CVE-2017-11317, CVE-2017-11357) nell’interfaccia grafica **Telerik**.

L’arsenale utilizzato dagli hacker, però, comprenderebbe anche una falla in **Microsoft SharePoint** (CVE-2019-0604) e una (CVE-2019-19781) in **Citrix**. Si tratta, come si deduce dall’anno di riferimento nei codici, di falle di sicurezza ben conosciute e per le quali sono disponibili patch e aggiornamenti.

Ma come mai emerge la pista che porta a Pechino? Stando all'analisi dei ricercatori, l'attribuzione degli attacchi, in realtà, è quasi impossibile. Buona parte degli exploit utilizzati, infatti, sfruttano porzioni di codice che sono circolate su Internet per molto tempo, mentre altri strumenti utilizzati per portare gli attacchi sono in realtà disponibili nei pacchetti software di pentesting.

Una traccia, viene sottolineato, emerge da un sample che alcuni motori antivirus individuano come **Korplug**, un malware utilizzato in passato da un gruppo **APT (Advanced Persistent Threat)** collegato al governo vietnamita. Il suo codice, però, è molto simile a **PlugX**, un "impianto" comparso per la prima volta nel 2008 proprio in una serie di attacchi attribuiti agli hacker cinesi.

Ed è proprio PlugX, secondo i ricercatori, a rappresentare l'indizio più pesante nei confronti di Pechino. Il malware, infatti, sarebbe utilizzato da almeno 10 gruppi APT, tutti

considerati al soldo del governo cinese.

Lo scenario, però, rimane abbastanza confuso. Tra gli strumenti utilizzati dai pirati per infiltrare i sistemi ci sono infatti anche alcune Web Shell, tra cui una versione (**HighShell**) che in passato è stata utilizzata dal gruppo iraniano **OilRig** e che è stata resa pubblica nell'aprile del 2019.

Insomma: l'impressione è che gli attacchi siano opera di un gruppo estremamente abile, che cerca di confondere le sue tracce utilizzando tecniche di depistaggio attraverso l'uso delle cosiddette "false flag", cioè l'utilizzo di strumenti normalmente usati da altri gruppi hacker.

Ora la palla passa agli esperti di sicurezza, che avranno il loro bel da fare per cercare di districare questa intricatissima matassa.

Condividi l'articolo

Cina: il software per pagare le tasse ha una backdoor. Spionaggio?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/06/29/in-australia-il-governo-lancia-lallarme-siamo-sotto-attacco/?utm_source=rss&utm_medium=rss&utm_campaign=in-australia-il-governo-lancia-lallarme-siamo-sotto-attacco