Le azioni di contrasto a TrickBot falliscono, ma il successo è a livello legale

Ott 15, 2020 Marco Schiaffino In evidenza, News, Scenario 0

L'azione di un consorzio di società di sicurezza ma ha solo "disturbato" la botnet, ma Microsoft ha registrato un precedente importante.

Non è la prima volta che le società di sicurezza "fanno squadra" per colpire una rete di cyber criminali. La vicenda, riportata da **ZDNet** in un articolo che ne riassume i caratteri principali, ha rilevanza per due motivi.

Il primo è che l'obiettivo del team di specialisti composto da esperti di sicurezza provenienti (tra gli altri) da **Microsoft**, **ESET** e **Symantec** era nientemeno che **TrickBot**, una delle botnet più longeve e pericolose in circolazione.

L'operazione non ha portato al risultato di smantellarne l'infrastruttura, ma secondo le testimonianze raccolte dai colleghi di ZDNet, questo "successo parziale" era ampiamente previsto. TrickBot, infatti, è una botnet molto strutturata e abbatterla con un singolo attacco sarebbe stato impensabile.

L'azione, però, ha permesso di mettere in difficoltà i cyber criminali che ne gestiscono l'attività, rallentandola e obbligandoli sulla difensiva. **Non solo: i protagonisti dell'operazione fanno notare anche che il parziale blocco di TrickBot ha avuto, come effetto collaterale, di minare alle fondamenta il mito della "intoccabilità" della botnet**.

In altre parole, l'azione congiunta delle società di sicurezza

ha portato, come conseguenza, un deterioramento della credibilità dei pirati informatici.

Il secondo elemento positivo è rappresentato da un dettaglio apparentemente secondario, che potrà però avere ripercussioni sulle future attività di chi lavora in ambito di cyber security.

Il provvedimento che ha autorizzato l'azione di contrasto a TrickBot ha infatti accolto un'istanza di Microsoft motivata dal fatto che il gruppo criminale avrebbe abusato del codice di Windows per scopi malevoli.

Il fondamento dell'autorizzazione a procedere, di conseguenza, è stato individuato nella semplice violazione del copyright relativo al software di Microsoft. Un precedente importantissimo, che renderà in futuro più agevole questo tipo di operazioni.

Secondo la giurisprudenza statunitense, infatti, questo tipo di violazione consente alla vittima di agire indipendentemente da considerazioni di giurisdizione nazionale.

In altre parole: se per dimostrare la competenza di un organo giurisdizionale prima era necessario rintracciare una vittima

che avesse la sua sede in un’area geografica all’interno della giurisdizione del giudice, da oggi questo requisito verrà considerato soddisfatto.

Di conseguenza, le azioni di contrasto alle attività dei cyber criminali saranno estremamente più “snelle” e potranno essere messe in campo senza dover passare per lungaggini burocratiche che richiedono testimonianze o analisi forensiche. Senza dubbio, una buona notizia.

Condividi l’articolo

Bug in Windows permette attacchi a catena sfruttando ICMPv6

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/15/le-azioni-di-contrasto-a-trickbot-falliscono-ma-il-successo-e-a-livello-legale/?utm_source=rss&utm_medium=rss&utm_campaign=le-azioni-di-contrasto-a-trickbot-falliscono-ma-il-successo-e-a-livello-legale

---

Bug in Windows permette attacchi a catena sfruttando

ICMPv6

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

La vulnerabilità è stata corretta con la tornata di aggiornamenti di ottobre, ma Microsoft teme che i primi attacchi possano arrivare a breve.

Nel corposo update rilasciato questo mese da Microsoft per i suoi sistemi operativi c'è una vulnerabilità che può mettere seriamente a rischio la sicurezza dei sistemi aziendali.

Il bug (CVE-2020-16898) riguarda la gestione dei collegamenti TCP/IP e, nel dettaglio, un problema a livello degli **ICMPv6 Router Advertisement**. Secondo quanto viene riportato sul sito Internet di Microsoft, un pirata informatico potrebbe inviare un pacchetto malevolo che avrebbe come risultato l'esecuzione di codice in remoto.

Non solo: la vulnerabilità consentirebbe di creare un worm in grado di propagarsi autonomamente all'interno della rete. Qualcosa di molto simile a quell'**EternalBlue** che ha creato non pochi problemi negli ultimi anni. **Non stupisce, quindi, che gli esperti di Microsoft abbiano assegnato alla falla di sicurezza un punteggio di criticità di 9.8 su 10**.

Il vero problema, a questo punto, non è tanto individuare la soluzione (la patch è già disponibile) quanto applicare gli aggiornamenti. Trattandosi di un componente fondamentale per il funzionamento delle reti aziendali, infatti, è prevedibile che gli amministratori IT si trovino a dover eseguire un buon numero di verifiche a livello di compatibilità prima di procedere all'update.

Insomma: quella che si apre è la classica "finestra di opportunità" che i cyber criminali raramente si lasciano scappare.

Per quanto riguarda le altre vulnerabilità emerse con la tornata di aggiornamenti di questo mese, 11 di queste sono identificate come "critiche".

La più pericolosa, per lo meno a livello di impatto che può avere, riguarda **Microsoft Outlook**. Il bug in questione (CVE-2020-16947) sfrutta la finestra di anteprima e permette, di conseguenza, di colpire la vittima anche se non apre il messaggio di posta elettronica infetto.

Per quanto riguarda l’ambiente cloud, invece, a preoccupare è la presenza di una falla a livello di **Microsoft Hyper-V** (CVE-2020-16891) che consentirebbe l’esecuzione di codice da un sistema guest al sistema host. In altre parole, sfruttando il bug sarebbe possibile infettare l’intero host partendo da una singola macchina virtuale ospitata al suo interno.

Condividi l’articolo

Le azioni di contrasto a TrickBot falliscono, ma il successo è a livello legale Tinexta crea il primo polo italiano della cyber security

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/14/bug-in-windows-permette-attacchi-a-catena-sfruttando-icmpv6/?utm_source=rss&utm_medium=rss&utm_campaign=bug-in-windows-permette-attacchi-a-catena-sfruttando-icmpv6

Tinexta crea il primo polo italiano della cyber security

Ott 14, 2020 Marco Schiaffino In evidenza, Mercato, News, Prodotto, RSS, Scenario 0

Tre acquisizioni e un progetto che punta a una forte crescita nel settore della sicurezza informatica secondo una formula tutta "Made in Italy".

Nasce il primo polo di cyber security tutto italiano. L'annuncio di **Tinexta**, gruppo nato nel 2009, riguarda una serie di acquisizioni nel settore cyber security che puntano a creare una business unit orientata all'erogazione di servizi e soluzioni di sicurezza informatica.

Le acquisizioni, nel dettaglio, riguardano la divisione "progetti e soluzioni" di **Corvallis**; la società di sicurezza **Yoroi** (che ha "in pancia" marchi come **Cybaze**, **Emaze** e **@Mediaservice.net**) e **Swascan**, azienda specializzata in piattaforme cloud di "security testing".

L'operazione porterà alla creazione di una business unit affidata alla gestione di **Marco Comastri**, già responsabile della funzione Sales & Marketing e Sviluppo Strategico di Tinexta.

Nel corso della conferenza stampa, il presidente del Gruppo Tinexta **Enrico Salza** ha sottolineato come la cyber security non rappresenti solo un settore in espansione dal punto di vista economico (il giro di affari stimato per il 2020 è di 120 miliardi di dollari) ma anche un fattore abilitante per la digitalizzazione nel nostro paese.

Una consapevolezza, quella della profittabilità del settore, condivisa anche dall'amministratore delegato **Pier Andrea Chevallard**.“I*n un momento di grande incertezza generale, Tinexta decide, con una chiara strategia, di raddoppiare la propria esposizione nel comparto digitale, affiancando alla propria BU Digital Trust la nuova BU Cybersecurity,* ***così portando il fatturato del Gruppo legato ad attività digitali a pesare circa il 55% del totale***” ha dichiarato Cehvallard. “*Sono fiducioso che la strategia di crescita perseguita, che farà leva anche sulla nostra posizione di leadership nel digital trust, consentirà di generare ulteriore valore per i nostri azionisti attraverso la rapida integrazione delle realtà acquisite e la complessiva maggiore esposizione ad un mercato in forte crescita*”.

Nel dettaglio, gli accordi di acquisizione prevedono l'acquisto del 70% del capitale della società contenente il ramo d'azienda di Progetti e soluzioni – IT e R&D4 di Corvallis, del 60% del capitale sociale di Yoroi S.r.l. e del 51% di Swascan, a fronte di un corrispettivo complessivo pari a 47,8 milioni di Euro.

Condividi l’articolo

Bug in Windows permette attacchi a catena sfruttando ICMPv6 Attacchi ai wallet Electrum Bitcoin fruttano 22 milioni di dollari ai pirati

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/14/tinexta-crea-il-primo-polo-italiano-della-cyber-security/?utm_source=rss&utm_medium=rss&utm_campaign=tinexta-crea-il-primo-polo-italiano-della-cyber-security

---

Attacchi ai wallet Electrum Bitcoin fruttano 22 milioni di dollari ai pirati

Ott 13, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

La tecnica è nota da almeno 2 anni, ma i cyber criminali hanno potuto continuare ad agire indisturbati rubando milioni alle loro vittime.

Due anni bastano per bloccare un attacco? Evidentemente no,

nemmeno quando ci sono in ballo milioni di dollari. La dimostrazione arriva da una vicenda che ha dell'incredibile e che viene riportata da **ZDNet** in un articolo pubblicato ieri.

Vittima degli attacchi sono gli utenti che utilizzano l'applicazione wallet di **Electrum** per gestire i loro conti in **Bitcoin**, che dal 2018 sono bersagliati da un gruppo di pirati informatici che sfrutta una vulnerabilità del circuito Electrum.

Come abbiamo raccontato in un articolo ormai due anni fa, il problema è legato alla struttura di server che gestisce le comunicazioni con i nodi Bitcoin. Il sistema Electrum, infatti, è stato pensato come un circuito aperto, all'interno del quale un singolo utente può inserirsi gestendo in proprio un server.

I pirati informatici, però, hanno trovato il modo di abusare di questa posizione utilizzando un semplice trucco di ingegneria sociale: visualizzare un pop up che propone un aggiornamento del software, il cui link però non punta al sito ufficiale, ma a **una versione malevola dell'applicazione**, programmata per trasferire tutti i fondi della vittima sui conti controllati dai criminali.

Per aggirare il sistema di autenticazione per l'autorizzazione al trasferimento, il programma visualizza una richiesta di codice **OTP (One Time Password)** al momento del primo avvio. Una procedura assolutamente anomala, ma che molti utenti non trovano particolarmente sospetta.

Dalle parti di Electrum hanno cercato di bloccare gli attacchi attraverso un sistema di filtri per individuare i server malevoli registrati su una blacklist e modificando le impostazioni per la visualizzazione dei pop up impedendo la visualizzazione di codice HTML.

Le contromisure, però, non sembrano aver funzionato. **Sui 10 conti utilizzati dai pirati per dirottare i fondi delle loro vittime ci sono oggi 1.980 Bitcoin, che al cambio attuale valgono più di 22 milioni di dollari**.

A quanto pare, però, il "colpo grosso" è stato messo a segno lo scorso agosto, quando i pirati hanno compromesso il wallet di un utente che aveva 1.400 Bitcoin (16 milioni di dollari) sul suo conto.

Condividi l'articolo

Raffica di attacchi hacker alle reti governative USA sfruttano Zerologon

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/13/attacchi-ai-wallet-electrum-bitcoin-fruttano-22-milioni-di-dollari-ai-pirati/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-ai-wallet-electrum-bitcoin-fruttano-22-milioni-di-dollari-ai-

pirati

RainbowMix: ecco come i pirati guadagnavano 150.000 dollari al giorno

Ott 09, 2020 Marco Schiaffino Hacking, In evidenza, News, RSS, Scenario, Tecnologia 0

La rete di app per Android è stata diffusa attraverso siti Internet e market paralleli. Nessun malware, ma semplici pubblicità per intascare milioni.

Se qualcuno avesse ancora dubbi sulle potenzialità economiche legate al cyber crimine, corra subito a leggersi il report (qui il collegamento) pubblicato in questi giorni da **White Ops**.

Il caso **RainbowMix**, descritto dagli autori dello studio **Gabi Cirlig**, **Michael Gethers**, e **Dina Haines**, non riguarda infatti un clamoroso data breach e nemmeno una campagna per la diffusione di pericolosi malware.

Si tratta di una semplice operazione che aveva come obiettivo la diffusione di applicazioni per sistemi Android in grado di visualizzare sui terminali delle pubblicità indesiderate attraverso una serie di tecniche che consentivano di occultare l'origine delle inserzioni.

Agli occhi dell'utilizzatore dello smartphone, infatti, le pubblicità sembrano essere visualizzate da applicazioni

assolutamente affidabili e conosciute come **YouTube** e **Chrome**. **In altre parole, gli utenti si trovavano sommersi di annunci senza poter capire quale fosse la loro effettiva origine**.

I pirati informatici che hanno ideato RainbowMix hanno utilizzato un’architettura simile a quella di un qualsiasi trojan, in cui le app agiscono seguendo i comandi inviati attraverso un **server Command and Control**, cui è affidato il compito di scegliere il circuito pubblicitario da utilizzare e la frequenza con cui visualizzare gli annunci.

Secondo quanto riporta lo studio di White Ops, la campagna ha consentito di ottenere in questo modo fino a **15 milioni di visualizzazioni** al giorno. Una stima approssimativa, basata su un profitto di un centesimo per impression, porterebbe l’incasso dei pirati a **150.000 dollari al giorno**.

Da un punto di vista tecnico, l’app non è particolarmente complessa e l’unica funzionalità “anomala” che sembra avere una certa importanza è quella che consente all’applicazione di sapere se lo schermo sia acceso o meno.

Altre funzioni individuate dai ricercatori, come la possibilità di registrare eventi come i boot di sistema, il collegamento all’alimentazione o modifiche nella connessione sembrano invece essere, a giudizio degli stessi analisti, semplice fumo negli occhi che ha il solo obiettivo di confondere chi analizza il funzionamento dell’applicazione.

Condividi l’articolo

BAHAMUT: il gruppo di mercenari al soldo di qualsiasi governo

---

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/10/09/rainbowmix-ecco-come-i-pirati-guadagnavano-150-000-dollari-al-giorno/?utm_source=rss&utm_medium=rss&utm_campaign=rainbowmix-ecco-come-i-pirati-guadagnavano-150-000-dollari-al-giorno

---

BAHAMUT: il gruppo di mercenari al soldo di qualsiasi governo

Ott 08, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, News, RSS, Scenario 0

I cyber-spioni sono specializzati in azioni mirate su bersagli sensibili, ma non disdegnano attività di disinformazione sul Web.

Professionisti del cyber spionaggio e della disinformazione di massa, disponibili a lavorare per il miglior offerente. È il gruppo **BAHAMUT**, così come lo descrivono i ricercatori di **BlackBerry** in un corposo report (qui il link per scaricarlo) in cui ne analizzano caratteristiche e tecniche di attacco.

Secondo gli analisti, i pirati sono specializzati in azioni in Asia e Medioriente sponsorizzate da enti governativi, ma non avrebbero un legame particolare con alcuna nazione: agirebbero principalmente come mercenari, offrendo i loro "servizi" al miglior offerente.

Gli episodi analizzati dai ricercatori comprendono attacchi a bersagli di alto profilo all'interno dei governi e del mondo

industriale di India, Emirati Arabi e Arabia Saudita, ma anche nei confronti di gruppi politici, organizzazioni non governative ed esponenti della società civile.

Un'attività, la loro, che viene portata avanti con estrema professionalità. Gli attacchi del gruppo BAHAMUT (il nome deriva da una leggenda araba e fa riferimento a un pesce mostruoso che sorreggerebbe sulla sua schiena il mondo – ndr) sfrutterebbero infatti strumenti estremamente evoluti, basati spesso **vulnerabilità zero-day**.

Stando a quanto si legge sul report, i ricercatori avrebbero collegato BAHAMUT anche a una decina di applicazioni malevole presenti sia su **Google Play**, sia su **App Store**.

Il loro modus operandi, inoltre, prevederebbe un'attenta pianificazione e quella che gli autori del report definiscono una "incredibile pazienza". In alcuni casi, infatti, i cyber-spioni avrebbero aspettato anche un anno per agire a colpo sicuro nei confronti di un bersaglio.

La loro attività non si limiterebbe però ad attacchi via malware o (preferibilmente) attraverso tecniche di phishing:

BAHAMUT avrebbe in catalogo anche la possibilità di portare avanti campagne di disinformazione a livello di opinione pubblica attraverso una capillare rete di siti Web in grado di distillare fake news.

L’esistenza di BAHAMUT rappresenta l’ennesima conferma di come si stia evolvendo il panorama dei gruppi APT (Advanced Persistent Threat) a livello globale. Se un tempo erano per lo più sezioni specializzate interne alle agenzie di servizi segreti, oggi agiscono sempre più spesso come freelance, disponibili a operare per chiunque.

Un fenomeno che interessa soprattutto aree del globo in cui agiscono governi con mire egemoniche a livello territoriale, ma che non hanno i mezzi o il know-how per dotarsi di un team di cyber spionaggio “in house”.

Condividi l’articolo

Fuorilegge i sistemi di spionaggio di Francia, Belgio e Regno Unito

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/08/bahamut-il-gruppo-di-mercenari-al-soldo-di-qualsiasi-governo/?utm_source=rss&utm_medium=rss&utm_campaign=bahamut-il-gruppo-di-mercenari-al-soldo-di-qualsiasi-governo

---

Fuorilegge i sistemi di spionaggio di Francia, Belgio e Regno Unito

Ott 07, 2020 Marco Schiaffino In evidenza, News, RSS, Scenario 0

La Corte di Giustizia Europea statuisce che la raccolta i dati è contraria alle normative dell'unione. Ammessa solo in casi di emergenza.

Stop alla raccolta indiscriminata di dati da parte di servizi segreti e agenzie di sicurezza. A deciderlo è stata la **Corte di Giustizia Europea**, che dopo 5 anni di procedimento ha stabilito che le attività di raccolta di informazioni su reti telefoniche e telematiche operate da **Francia**, **Belgio** e **Regno Unito** violano le norme comunitarie.

La sentenza, consultabile a questo indirizzo, precisa che la tutela della confidenzialità delle comunicazioni e del traffico dati non può essere violata se non all'interno dei

principi di proporzionalità che ispirano i trattati comunitari.

In altre parole: l’obbligo per operatori telefonici e fornitori di accesso a Internet di trasmettere i dati del traffico e delle comunicazioni a enti governativi è illegale.

Il quadro a cui si applica la decisione è quello adottato dai tre stati in cui le informazioni vengono memorizzate in database e conservate a tempo indeterminato per poi essere utilizzate in caso di necessità.

Esattamente come nella prima fase del **Datagate**, il tema è legato alla gestione dei **metadati**, le informazioni registrate dalle società di telecomunicazione che, una volta elaborati con algoritmi di intelligenza artificiale, consentono in pratica di tracciare qualsiasi attività e relazione sociale dei cittadini.

Insomma: si tratta di qualcosa di molto simile a ciò che ha messo a nudo **Edward Snowden** negli Stati Uniti, ma che nell’Unione Europea **confligge frontalmente** con la legislazione

in tema di privacy.

Una considerazione che è stata alla base anche di un'altra decisione della Corte Europea, che lo scorso 16 luglio ha dichiarato illegale il **Privacy Shield**, l'accordo tra UE e **Stati Uniti** che consentiva la conservazione e il trattamento dei dati dei cittadini europei sul territorio statunitense.

Insomma: la decisione segna un punto a favore di **Privacy International**, l'associazione britannica che ha avviato la causa e che adesso può esultare per una decisione che permetterà di rendere più stringenti le norme a tutela della privacy per i cittadini europei.

Per gli attivisti, però, rimane il boccone amaro di sapere che proprio la Gran Bretagna sarà il paese su cui impatterà meno la decisione della Corte. Con l'approssimarsi della **Brexit**, infatti, è probabile che il governo di Londra non si debba preoccupare troppo delle possibili ripercussioni.

Condividi l'articolo

Il chip di sicurezza T2 di Apple a rischio attacco?

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/07/fuorilegge-i-sistemi-di-spionaggio-di-francia-belgio-e-regno-unito/?utm_source=rss&utm_medium=rss&utm_campaign=fuorilegge-i-sistemi-di-spionaggio-di-francia-belgio-e-regno-unito

Il chip di sicurezza T2 di Apple a rischio attacco?

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

L'allarme circola in rete da qualche giorno e riguarda un attacco che permetterebbe di eseguire un jailbreak del co-processore. A rischio la sicurezza di macOS.

Per il momento gli esperti di sicurezza non si sbilanciano sull'applicabilità della tecnica di attacco, ma se dovesse essere confermata potrebbe trattarsi di una vera mazzata per la sicurezza dei computer **Apple**.

A finire nel mirino, infatti, è il chip di sicurezza **T2**, il co-processore che viene montato su tutti i computer con sistema **macOS** e a cui sono affidati, oltre alla gestione di alcuni servizi a basso livello, anche la gestione di dati sensibili come le chiavi crittografiche, le password di **Accesso Portachiavi**, il riconoscimento del Touch ID e la crittografia dei dischi.

Il chip T2 è stato introdotto nel 2017 e rappresenta uno dei classici strumenti di security basati sull'hardware. L'idea, in pratica, è quella di confinare tutti i dati sensibili in un chip distinto dal processore centrale er poterli proteggere meglio.

La comparsa di una vulnerabilità in grado di eseguire codice all'interno del chip T2 (qui è possibile leggere un report a riguardo pubblicato da **ironPeak**) di conseguenza ha

immediatamente messo in allarme buona parte del mondo della sicurezza informatica.

Ma come funzionerebbe l’attacco? In pratica, sfrutterebbe due exploit ideati per il jailbreak dei sistemi **iOS**. Le due tecniche, chiamate **Checkm8** e **Blackbird**, deriverebbero la loro efficacia dal fatto che alcuni componenti hardware del chip sarebbero uguali a quelli usati nell’**iPhone**.

L’attacco, in ogni caso, richiede un accesso fisico al computer e in particolare un collegamento attraverso un cavo USB-C nella fase di avvio del computer utilizzando **Checkra1n** versione 0.11.0, un software per il jailbreaking piuttosto conosciuto.

Insomma: qualcosa che esclude (almeno per il momento) la possibilità di attacchi in remoto ma che apre la strada a tecniche di attacco hardware, spesso utilizzate da servizi segreti e gruppi APT.

Secondo i ricercatori, infatti, sarebbe possibile implementare l’attacco in modo che si avvii automaticamente al momento

della connessione di un dispositivo o di un semplice cavo USB-C modificato ad arte per eseguire il jailbreak.

A rendere più spinosa la questione, c'è il fatto che la vulnerabilità non potrebbe essere corretta tramite un semplice aggiornamento, ma richiederebbe l'installazione ex novo di **BridgeOS**, il sistema operativo che gestisce il co-processore T2.

Condividi l'articolo

Invisibili per 9 anni: ESET accende i riflettori sul gruppo XDSpy

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/06/il-chip-di-sicurezza-t2-di-apple-a-rischio-attacco/?utm_source=rss&utm_medium=rss&utm_campaign=il-chip-di-sicurezza-t2-di-apple-a-rischio-attacco

---

Invisibili per 9 anni: ESET accende i riflettori sul gruppo XDSpy

Ott 05, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario 0

I cyber-spioni sarebbero attivi dal 2011, ma sarebbero riusciti a passare completamente inosservati fino a qualche mese fa.

Non capita spesso di individuare un nuovo protagonista nel panorama degli **APT (Advanced Persistent Threat)**, i gruppi hacker che lavorano per conto di governi e servizi segreti. Più raro che mai è che i "nuovi arrivati" abbiano alle spalle quasi un decennio di attività nel settore del cyber-spionaggio.

Secondo i ricercatori di **ESET**, però, il gruppo battezzato come **XDSpy** sarebbe attivo fin dal 2011 e le loro operazioni sarebbero passate sottotraccia fino all'inizio del 2020, quando gli analisti si sono imbattuti in un malware che hanno definito "non particolarmente sofisticato".

Nel loro report, i ricercatori spiegano che **XDDown** è un trojan modulare che integra diverse funzionalità: dalla raccolta di informazioni sul sistema, al furto di documenti e password, fino al tracciamento degli spostamenti attraverso il rilevamento delle connessioni alle reti Wi-Fi pubbliche.

Anche se il malware utilizzato dai pirati non è particolarmente complesso, i ricercatori di ESET hanno ricostruito parte dell'attività del gruppo, che avrebbe interessato principalmente l'Europa orientale e i Balcani. **Nel dettaglio, gli hacker di XDSpy avrebbero colpito in Bielorussia, Moldavia, Russia, Serbia e Ucraina**.

Il vettore di attacco utilizzato nelle campagne più recenti sarebbe rappresentato da classiche email di phishing, in buona parte facenti riferimento alla pandemia da **Covid-19**. Qualcosa di non molto originale, ma che evidentemente mantiene una sua efficacia.

La definizione di APT deriverebbe invece dal loro modus operandi, che secondo gli analisti avrebbe privilegiato l'offuscamento alla persistenza. In altre parole, il malware utilizzato da XDSpy integra alcune funzioni come l'eliminazione di alcuni plugin dopo un certo periodo di tempo che denota una maggiore attenzione alla necessità di rimanere "invisibili".

Difficile capire quale sia la "paternità" del gruppo. Nel loro report, gli analisti rilevano come l'area di azione sia considerata normalmente appannaggio sia dei paesi facenti parte della **NATO** (con gli **Stati Uniti** come primi indiziati) sia del governo di Mosca.

Condividi l'articolo

MosaicRegressor: adesso il trojan si nasconde dentro UEFI

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/10/05/invisibili-per-9-anni-eset-accende-i-riflettori-sul-gruppo-xdspy/?utm_source=rss&utm_medium=rss&utm_campaign=invisibili-per-9-anni-eset-accende-i-riflettori-sul-gruppo-xdspy

MosaicRegressor: adesso il trojan si nasconde dentro UEFI

Ott 05, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario, Tecnologia 0

Viene descritto come un "impianto" nel cuore del sistema. Secondo gli esperti di Kaspersky potrebbe essere stato sviluppato da un gruppo cinese.

Anche se non è il primo caso, la scoperta di un malware che agisce a livello del **UEFI** (Unified Extensible Firmware Interface) è comunque qualcosa di estremamente raro.

L'utilizzo di un malware in grado di agire a livello UEFI

rappresenta infatti una minaccia particolarmente insidiosa a livello di persistenza. La sua presenza, infatti, non può essere contrastata nemmeno con la formattazione del disco.

Non stupisce, di conseguenza, che il caso di **MosaicRegressor** abbia attirato l'attenzione dei ricercatori di **Kaspersky**, che in un corposo report pubblicato sul blog ufficiale della società sicurezza ne analizzano caratteristiche e (probabile) origine.

Nel dettaglio, i ricercatori hanno individuato una serie di componenti "sospetti" all'interno di un'immagine UEFI, alcuni dei quali sembrano essere derivati da quelli sviluppati da **Hacking Team** (un'azienda italiana produttrice di spyware – ndr) per alcuni dei suoi "impianti".

L'esemplare individuato dagli analisti di Kaspersky, nonostante alcuni similitudini con i malware sviluppati dall'azienda italiana, hanno delle caratteristiche uniche che fanno pensare a una variante di una piattaforma battezzata con il nome di MosaicRegressor.

Il malware, spiegano i ricercatori, è composto da diversi moduli che interagiscono tra loro e hanno le funzionalità classiche di un trojan: dal recupero di informazioni sul sistema infetto al furto dei documenti memorizzati sul dispositivo.

Stando alle indagini condotte, il malware sarebbe stato utilizzato a partire dal 2017 e le vittime confermate comprenderebbero anche sedi diplomatiche in Africa, Asia ed

Europa.

Per quanto riguarda l’attribuzione degli attacchi, dalle parti di Kaspersky non si sbilanciano troppo, ma alcuni degli indizi individuati fanno pensare a un autore asiatico e, in particolare, a qualcuno che abbia un legame con la Cina.

L’individuazione di MosaicRegressor, in ogni caso, è la conferma di un fenomeno in crescita che vede i gruppi APT (Advanced Persistent Threat) prendere di mira BIOS e UEFI per garantirsi un livello di persistenza elevato sulle macchine compromesse.

Condividi l’articolo

Invisibili per 9 anni: ESET accende i riflettori sul gruppo XDSpy Il Perimetro di sicurezza cibernetica: la lunga strada per la protezione di reti e sistemi nazionali

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/10/05/mosaicregressor-adesso-il-trojan-si-nasconde-dentro-uefi/?utm_source=rss&utm_medium=rss&utm_campaign=mosaicregressor-adesso-il-trojan-si-nasconde-dentro-uefi