Perimetro cibernetico, top secret il nome di aziende ed enti strategici

Sarà top secret l'elenco degli enti pubblici, delle aziende statali e private che saranno inseriti nel perimetro di sicurezza nazionale cibernetica. La lista sarà completata entro la fine del mese e sarà composta da almeno 150 nominativi: rappresentano gli asset strategici dell'Italia, le infrastrutture critiche da difendere con un "scudo" governativo dagli attacchi informatici. E saranno individuati dai ministeri secondo i criteri stabiliti dal DPCM del 30 luglio 2020 ora pubblicato in Gazzetta Ufficiale ed in vigore dal 5 novembre prossimo.

"Negli ultimi trentasei mesi è stato avviato un processo di adeguamento normativo volto a potenziare la resilienza del Paese. Con la legge sul Perimetro, l'Italia si è posta all'avanguardia dell'Europa", ha dichiarato **Gennaro Vecchione**, il direttore del Dis cui è assegnato il compito di coordinare l'attuazione del Perimetro di sicurezza cibernetica.

In quali settori è possibile scegliere i soggetti che esercitano funzioni e servizi essenziali?

"Ai fini dell'inclusione nel perimetro", si legge nel decreto, *"sono oggetto di individuazione soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR (Comitato interministeriale per la sicurezza della Repubblica), nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti*

settori di attività, ove non ricompresi in quello governativo:

a) interno;

b) difesa;

c) spazio e aerospazio;

d) energia;

e) telecomunicazioni;

f) economia e finanza;

g) trasporti;

h) servizi digitali;

i) tecnologie critiche

Quale processo si attiva in caso di incidente o attacco informatico?

Nel caso di incidente, spiega Repubblica, l'azienda violata è tenuta a informare, entro 6 ore al massimo (e non, come previsto dalla direttiva europea Nis, entro le 24 ore successive dal malfunzionamento) il **Csirt** (Computer security incident response team) cioè il gruppo di esperti istituito presso il Dis. Quando l'intrusione è grave, si attiva il Nucleo per la sicurezza cibernetica, che propone al presidente del Consiglio delle ipotesi di risposta all'attacco e coordina il ripristino del servizio.

Il Nucleo per la sicurezza cibernetica è composto da tutti gli attori nazionali dell'architettura cyber: delegati del Dis, di Aise e Aisi, dei ministeri, dell'Agenzia per l'Italia digitale, della Protezione Civile, della Postale e il consigliere militare del premier.

I soggetti inseriti nel perimetro di sicurezza nazionale cibernetica rischiano sanzioni fino a 1,5 milioni di euro se non comunicano l'incidente o attacco informatico.

Per approfondire:

- ***Leggi sulla Gazzetta Ufficiale il Regolamento in materia di perimetro di sicurezza nazionale cibernetica***

The post Perimetro cibernetico, top secret il nome di aziende ed enti strategici appeared first on Key4biz.

https://www.key4biz.it/perimetro-cibernetico-top-secret-il-nome-di-aziende-ed-enti-strategici/327013/

Rapporto Enisa 2020, il panorama della cybersecurity in Europa in 22 ebook (e un video)

Il 2020 è iniziato sotto il segno della pandemia di Coronavirus ed è continuato sotto il segno dell'emergenza sanitaria, con i cyber criminali che non hanno perso tempo per sfruttare la crisi e rendere i propri attacchi informatici sempre più mirati e dannosi.

L'Agenzia europea per la sicurezza delle reti e dell'informazione (**Enisa**) ha pubblicato l'edizione 2020 del ***Threat landscape Report***, con l'obiettivo di delineare il panorama delle principali minacce informatiche nell'Unione europea nel periodo gennaio-aprile 2020.

Un’indagine che è stata strutturata in maniera modulare, cioè composta da **22 mini rapporti, disponibili come ebook o in formato pdf**, ognuno dedicato ad un aspetto specifico della cybersicurezza europea: dalle principali minacce (come malware, spam, phishing, DDoS, furto di identità) alle novità nel campo della cyber threat intelligence, fino all’analisi approfondita degli incidenti più rilevanti nel 2020 relativi all’Europa e il Nord America.

Le principali cyber minacce

Tra le minacce principali del primo semestre dell’anno in corso troviamo al primo posto i ***malware***, seguiti dagli attacchi *web-based*, con il ***phishing*** a chiudere il podio.

Seguono gli attacchi *web-app*, il classico spam, i tradizionali **DDoS** o *Distributed Denial of Service*, il **furto d’identità**, il ***data breach***, l’*insider threat* e a chiudere la Top Ten le ***botnet***.

Tra i primi 20 posti troviamo anche i temibili ***ransomware***, il cyber spionaggio e il ***cryptojacking***.

La gran parte di questi attacchi mira sempre alla massimizzazione dei profitti e alla sottrazione illecita di dati sensibili, codici e credenziali, personali, aziendali e relativi/e alla salute, i conti in banca e la nostra identità. Tra gli obiettivi anche la proprietà intellettuale e i documenti governativi.

In particolare, si legge nello studio, è **aumentato di molto il numero delle vittime di phishing in Europa**, frutto di **campagne fraudolente legate al Covid-19** che hanno attirato un gran numero di ignari utenti.

Gli attacchi a tema Covid-19 includono messaggi con allegati o link che hanno un unico obiettivo: reindirizzare gli utenti a siti di phishing o spingergli a scaricare malware sui propri device.

La spesa delle aziende in cybersecurity

Secondo un nuovo studio condotta da Kaspersky, invece, **la spesa in cybersecurity è cresciuta dal 23 al 26% tra le piccole e medie aziende, nell'ultimo anno, e dal 26 al 29% tra le grandi aziende**.

Il 71% delle imprese ha comunque dichiarato di voler accrescere ulteriormente gli investimenti in sicurezza

informatica e digitale nei prossimi tre anni: +11% per le organizzazioni più grandi e +12% per quelle medio-piccole.

In questo caso, stando ai dati dell'IT Security Calculator, tra le principali minacce alla cybersecurity globale delle imprese, troviamo che nel 45% dei casi si parla di fuga di dati, nel 43% di virus e malware, nel 42% dei casi di violazione delle politiche di sicurezza IT da parte dei dipendenti.

Attacchi *phishing*, *cryptomalware*, *ransomware* e DDoS rappresentano, invece, tra il 34 ed il 36% delle cyber minacce più diffuse.

> *Rapporto Enisa 2020, il panorama della cybersecurity in Europa in 22 ebook (e un video)*

Mirai, quattro nuove varianti del malware minano la sicurezza dei dispositivi IoT

I ricercatori dell'Unità 42 di Palo Alto Networks hanno esaminato quattro varianti Mirai operanti in due campagne scoperte di recente e che sfruttano come veicoli di diffusione due exploit per IoT.

Mirai è un malware implementato per operare su dispositivi connessi a Internet, in particolare su diverse piattaforme

utilizzate nei dispositivi IoT, rendendoli parte integrante di una botnet usata per attacchi informatici su larga scala. Infatti l'infrastruttura Mirai, scoperta per la prima volta nel 2016 è stata ampiamente utilizzata per sferrare imponenti tipologie di attacchi DDoS.

I due exploit IoT

In entrambi gli exploit rilevati è il tool comune *wget (usato* per gestire i server Linux in remoto tramite sessione ssh) a rappresentare il mezzo di propagazione di diversi binari Mirai compilati per essere eseguiti su diverse architetture. Nello specifico tale utilità viene richiamata per scaricare uno shell script dall'infrastruttura malevola, sfruttando un mancato processo di sanificazione di alcuni parametri HTTP utilizzati.

Nel primo exploit un command injection viene adoperato durante il processo di impostazione di un server Web NTP (Network Time Protocol**)** per la sincronizzazione dell'ora. In questo caso il servizio non riesce a disinfettare il valore del parametro HTTP NTP_SERVER, che quindi può portare all'esecuzione di comandi arbitrari e quindi al download di un binario Mirai compatibile.

A tal proposito, l'analisi condotta ha trovato nei firmware di alcuni dispositivi IoT (per alcuni dei quali i fornitori non forniscono più supporto) diverse routine di gestione NTP vulnerabili per la sincronizzazione dell'ora tramite HTTP.

Il secondo exploit per il quale i ricercatori hanno ricavato però meno informazioni, potrebbe invece consentire un command injection arbitrario, sfruttando una mancata sanificazione del parametro HTTP pid di un non meglio specificato servizio mirato (probabilmente uno strumento di gestione di processi remoti).

Le quattro nuove varianti Mirai

Tutte e quattro le varianti Mirai, possiedono delle funzionalità atte a sferrare attacchi DDoS e sfruttano come metodo di consegna i due exploit rilevati, come di seguito riportato:

- le varianti Mirai 1 e 2 utilizzano come metodo di consegna l'exploit 1;
- le varianti Mirai 3 e 4 utilizzano come metodo di consegna l'exploit 2;

Tra queste varianti la numero quattro, affermano i ricercatori, rappresenta la minaccia più pericolosa, possedendo altre caratteristiche di infezione non presenti nelle altre:

- sfrutta gli exploit già utilizzati nelle passate varianti;
- sfrutta ulteriori vulnerabilità per infettare gli host vulnerabili:

Android debug bridge shell, CVE-2019-14931, Fastweb Fastgate RCE, ASUS RT-AC66U RCE, HomeMatic Zentrale CCU2 RCE, EnGenius RCE, CVE-2013-2251, CVE-2015-1187, Netlink GPON Router RCE, ThinkPHP RCE, D-Link Router RCE, CVE-2020-5722, Vacron NVR RCE, CVE-2019-16920, CVE-2019-10655, Netgear RCE, CVE-2020-8515, CVE-2017-18377, Edimax EW-7438RPn RCE, CVE-2020-1956, CVE-2018-17173, CVE-2019-19356, 3Com OfficeConnect RCE, CVE-2018–13023, NUUO NVRmini RCE, CVE-2019-7276, CVE-2018-19276, CVE-2011-3587, Multiple IoT RCE, CVE-2016-6277, Sar2HTML RCE, CVE-2018-7841, CVE-2019-16057, CCTV-DVR RCE.

La sicurezza IoT, un problema da

risolvere

Pertanto la crescente diffusione di dispositivi IoT, non solo nello smart home ma anche nel settore industriale e le previsioni che ne stimano, nei prossimi anni, un ulteriore e considerevole incremento (cresce la mole di dati da gestire e il numero di applicazioni che dovranno essere sviluppate) rendono, oramai, il tema della sicurezza IoT un serio problema la cui soluzione non può più essere rimandata.

Per saperne di più: IoT
Mirai, quattro nuove varianti del malware minano la sicurezza dei dispositivi IoT

Cybercrime, 13 app contenenti Adware trovate sul Play Store di Google

Una nuova famiglia di adware è stata trovata in applicazioni disponibili sul Play Store di **Google**.

13 app con Adware

Lo rendono noto i ricercatori di **Bitdefender** in un recente post. Anche se non è una novità imbattersi in app in bundle con adware, in questo caso le 13 applicazioni scoperte, appartenenti alla categoria di utility comuni (quali lettori

di musica e video, downloader e aggregatori di social media) e che propinano annunci altamente persistenti, sono accompagnate anche da oltre 1.000 recensioni positive che si sono rilevate in realtà false e provenienti potenzialmente dagli account fittizi della stessa rete di bot spam con il solo scopo di ottenere una più ampia diffusione con un maggior numero di download.

L'analisi condotta dai ricercatori di sicurezza oltre che aver trovato delle evidenze che potrebbero ricondurre tutte a un singolo sviluppatore, ha anche rivelato, in buona parte dei campioni analizzati, una particolare funzionalità SDK deputata a ottenere delle autorizzazioni intrusive per la privacy e che consentirebbero alle app di leggere notifiche, raccogliere dettagli di contatto, messaggi di testo e codici OTP per le autorizzazioni a più fattori (MFA).

Le evidenze

Diverse sono le evidenze che portano a pensare a un unico sviluppatore, anche se le app risultano pubblicate da nove differenti soggetti. Ciò potrebbe essere, in realtà, un escamotage per evitare un'eventuale rimozione qualora venisse rilevato un qualunque comportamento indesiderato riconducibile allo stesso sviluppatore.

Alcune coincidenze sono rappresentate dagli schemi molto simili negli indirizzi email usati per il contatto di supporto e le politiche sulla privacy, altre dallo stesso modello/format dei certificati di firma. Tutte le norme sulla privacy sono inoltre ospitate sullo stesso dominio "sites.google.com".

Da un punto di vista strutturale del codice, le applicazioni presentano tutte lo stesso meccanismo di offuscamento e di crittografia delle stringhe. In particolare l'offuscamento viene applicato sia al codice vero e proprio dell'app che alla componente adware che concentra la sua attività nella

visualizzazione di annunci Google e Facebook.

Un’ulteriore somiglianza infine si rileva nell’interfaccia utente delle app. Molte di loro condividono le stesse caratteristiche visive oltre che la stessa struttura.

Analisi del codice

L’analisi del codice condotta su una di queste applicazioni (“launchserfor.apps”), scelta perché presentava la maggior parte delle funzionalità SDK e risultava ancora disponibile sul Play Store al momento dello studio, ha rilevato principalmente che:

- Il codice è fortemente offuscato e le stringhe utilizzate vengono crittografate attraverso l’algoritmo di crittografia DES;
- in una versione di prova iniziale dell’adware, è stato scoperto che era stata invertita la funzione dei pulsanti “Accetta” e “Rifiuta” al momento della richiesta da parte dell’app di accedere alle notifiche;
- la versione SDK ha il codice per chiedere l’autorizzazione a leggere tutte le notifiche ed inviarle tempestivamente ad un server C2 (hxxps: //t.lineranalysis.com/api/ APClient3/);
- l’app invia anche informazioni generiche al server C2 come l’elenco delle applicazioni installate, l’ID Android del dispositivo, il nome del pacchetto, il tipo di rete, l’operatore sim, file di registro, timestamp e controlli di stato.

Telemetria e attribuzione

La telemetria che ha individuato una diffusione della campagna più marcata principalmente in India, Corea e Stati Uniti, mostra anche una presenza significativa in paesi europei trai i quali l’Italia.

Sebbene non si possa avere certezza assoluta, diversi elementi quali la lingua in uso nella maggior parte delle pagine sulla privacy e dei file log e la provenienza dei registrar di tutti i server C2 coinvolti riconducibile alla società Alibaba Cloud Computing, inducono ad attribuire la paternità della campagna a sviluppatori cinesi.

Adware: perchè fare attenzione

Come evidenziato dai ricercatori, anche se un adware aggressivo solitamente potrebbe non essere nocivo quanto un malware, la sua attività potrebbe comunque influire negativamente sull'esperienza complessiva dell'utente con il proprio dispositivo oltre che sulle prestazioni della batteria.

Risulta pertanto fondamentale evitare, in genere, di esporre i propri dispositivi a minacce online di qualsiasi natura (frodi, phishing, scam) utilizzando una soluzione di sicurezza adeguata anche per i dispositivi mobile (non solo desktop) e scaricando sempre le app dagli store ufficiali (che restano sempre e comunque i marketplace più sicuri e affidabili) prestando particolare attenzione alla veridicità e attendibilità delle recensioni prima di avviare qualsivoglia installazione.

Maggiori dettagli sugli IoC e sull'elenco completo delle app identificate durante l'indagine e segnalate, in modo responsabile e in tempi utili, al team di sicurezza di Google sono reperibili sul sito **Bitdefender**.

Qualora ci si accorgesse di aver installato una di queste applicazioni, si raccomanda di provvedere alla sua disinstallazione il prima possibile.

https://www.key4biz.it/cybercrime-13-app-contenenti-adware-trovate-sul-play-store-di-google/325932/

Bando Ue cybersecurity da 10 milioni di euro, c’è tempo fino al 5 novembre

La Commissione europea ha lanciato quest’estate una nuova **call per la cybersecurity** negli Stati membri dell’Unione con una **dotazione complessiva di 10,5 milioni di euro**.

Il bando è parte del Connecting Europe Facility (CEF) Telecom, il programma gestito da **INEA (Innovation and Networks Executive Agency della Commissione europea)** per lo sviluppo di infrastrutture di servizio digitali (DSIs) e network per la banda larga.

Come ha spiegato Thierry Breton, Commissario per il Mercato interno, in occasione del lancio dell’iniziativa: “*La call contribuirà a rafforzare la nostra resilienza contro le minacce informatiche in linea con le nostre ambizioni digitali e con la nostra strategia globale, che comprende il regolamento sulla cibersicurezza, la direttiva NIS e le raccomandazioni del programma di cibersicurezza*”.

Un sostegno a progetti concreti nel settore della sicurezza informatica, che nelle intenzioni della Commissione: “*Contribuirà anche a far progredire le tecnologie e le soluzioni innovative di cybersecurity in modo mirato*”.

Le proposte inviate saranno valutate tra novembre 2020 e gennaio 2021, mentre la selezione finale dei progetti vincitori potrebbe avvenire tra aprile e maggio sempre del

2021.

Il bando coprirà diversi ambiti di intervento: dalla protezione fisica e virtuale delle infrastrutture della trasformazione digitale ad un più efficace coordinamento nella risposta ai cyber incidenti.

> *Bando Ue cybersecurity da 10 milioni di euro, c'è tempo fino al 5 novembre*

Il Dipartimento di Giustizia USA contro le criptovalute: "Una minaccia alla sicurezza nazionale". Il Documento

Le **criptovalute** e, più in generale, le tecnologie ad esse correlate, come la *distributed ledger technology*, potrebbero favorire una trasformazione dei dispositivi finanziari che regolano le transazioni commerciali e rendere più efficiente l'attuale sistema economico.

Allo stesso tempo, però, in assenza di obblighi informativi e di regole di trasparenza, le piattaforme di scambio sono altresì esposte a elevati rischi operativi e di sicurezza.

A differenza degli intermediari autorizzati, queste piattaforme non sono tenute ad alcuna garanzia di qualità del

servizio, né devono rispettare requisiti patrimoniali o procedure di controllo interno e gestione dei rischi, con conseguente elevata probabilità di frodi ed esposizione al cyber crimine.

Il documento del Dipartimento di Giustizia americano

A riguardo, il **Dipartimento di Giustizia degli Stati Uniti** ha diffuso un Rapporto dal titolo "***Cryptocurrency: An Enforcement Framework***", realizzato dalla *Cyber-Digital Task Force*, con l'obiettivo di fornire una panoramica esaustiva delle principali minacce conosciute ed emergenti provenienti dall'utilizzo delle criptomonete.

"*E' di vitale importanza che la criptovaluta non metta in pericolo la nostra sicurezza pubblica e la nostra sicurezza nazionale, lo è per gli Stati Uniti, lo è per i nostri alleati*", si legge nel comunicato del Dipartimento.

Come ha spiegato il direttore dell'FBI, **Christopher Wray**: "*Le criptovalute sono utilizzate in maniera diffusa dei cyber criminali che sfruttano attacchi ransomware per guadagnare soldi facili in maniera illecita, perché è uno strumento finanziario che offre loro anonimato, gli permette di nascondere la loro vera identità*".

Non un documento necessariamente "*contro*" questo nuovo modello di valuta virtuale, ma una richiesta di maggiore attenzione da parte delle autorità regolatorie.

"*Le criptovalute e le distributed ledger technologies portano con sé non solo minacce, ma anche vantaggi operativi di non poco conto* – ha affermato **Brian C. Rabbit**, membro della Task Force – *ma in assenza di un quadro giuridico preciso, rimane impossibile attuare un'efficace tutela legale e/o contrattuale degli utenti".*

Utenti che possono, pertanto, trovarsi esposti a dover subire ingenti perdite economiche, ad esempio in caso di condotte fraudolente, fallimento o cessazione di attività delle piattaforme online di scambio, presso cui vengono custoditi i portafogli digitali personali.

Criptovalute e cyberminacce

Il documento si compone di tre parti principali. Nella prima si elencano alcuni esempi di utilizzi illeciti delle criptomonete, come transazioni finanziarie condotte in maniera illegale, riciclaggio di denaro sporco, furti e frodi.

Secondo uno studio CipherTrace, del 2019, l'utilizzo di criptovalute per furti, frodi e raggiri è cresciuto del +150% in un anno. Solo per farsi un'idea del volume di guadagni criminali che si può generare con l'utilizzo di queste monete virtuali, grazie allo schema piramidale detto "*Plus Token*", sono stati rubati 2,9 miliardi di dollari.

La seconda parte prende in considerazione, invece, gli strumenti legali e regolatori a disposizione del Governo, delle Istituzioni e delle Authority per contenere le attività illecite che ruotano attorno alle criptovalute, mettendo in evidenza la crescente partnership tra Dipartimento di Giustizia, Securities and Exchange Commission, Commodity Futures Commission e diverse agenzie all'interno il Dipartimento del Tesoro.

Un'ultima parte, infine, è dedicata alla valutazione dello scenario attuale, con alcune indicazioni relative ai passi da compiere, da qui in poi, per regolare questo settore e allo stesso tempo garantire l'utilizzo di strumenti finanziari nuovi senza lasciar spazio d'azione ai cyber criminali.

> *Il Dipartimento di Giustizia USA contro le criptovalute: "Una minaccia alla sicurezza nazionale". Il Documento*

Cybercrime, come funziona un attacco side channel

Fu il ricercatore **Paul Kocher** a parlare per la prima volta di attacco su canale laterale negli anni ’90 in occasione dell’RSA Data Security and crypto conferences, dove mostrò che era possibile ottenere informazioni (propedeutiche per un attacco informatico) sull’implementazione di un sistema di sicurezza senza sfruttare una particolare vulnerabilità del crittosistema dal punto di vista matematico quanto piuttosto un aspetto secondario che nessuno, fino ad allora, aveva considerato: il tempo di esecuzione delle operazioni algoritmiche.

Da allora, con il termine SCA (Side Channel Attack) viene indicato un qualsiasi exploit di sicurezza che implica una raccolta indiretta di informazioni sull’attività di un dispositivo, utilizzata successivamente per violare il dispositivo stesso.

Attacco side channel, come funziona

A differenza di molti altri tipi di exploit di sicurezza, gli attacchi side channel non sfruttano vulnerabilità hardware o software, ma osservano piuttosto il modo in cui il software di base del dispositivo accede all’hardware, alla ricerca di un canale secondario che possa dare preziose indicazioni per la ricostruzione dei dati di elaborazione.

Gli attacchi side channel possono dunque colpire qualsiasi

sistema operativo Windows, Linux e Mac.

Le famose vulnerabilità riscontrate, negli ultimi anni, nei processori moderni denominate **Meltdown, Spectre e Fallout** ne sono un esempio lampante.

Ma ancora prima che il termine entrasse in uso negli anni ‘90 già si parlava di intercettazioni phreaking di Van Eck e tecniche simili ovvero di particolari forme di attacchi che oggi avremmo considerato come declinazioni SCA.

Le tipologie degli SCA

Tutti gli attacchi side channel sfruttano i cambiamenti subiti, durante l’attività operativa del dispositivo target, da una serie di proprietà del canale secondario prescelto, come ad esempio il calore generato, il consumo di energia o il tempo di esecuzione.

Diversi possono essere, infatti, i parametri di misura analizzati sui canali laterali da utilizzare per sferrare attacchi SCA:

- L’analisi dei tempi di risposta dei processori (timing attack) o degli accessi alla cache (cache attack) per tracciare il movimento dei dati tra CPU e la memoria di un sistema. L’affidabilità di questi attacchi punta sul fatto che l’esecuzione degli algoritmi spesso dipendono dai dati di input immessi e pertanto in base alle statistiche ottenute è possibile estrapolare delle fughe di informazioni;
- l’analisi di risposta del processore ad una serie di errori di calcolo studiati ad hoc (differential fault attack);
- l’analisi dei suoni prodotti dalla CPU per decodificare l’attività operativa dell’unità di elaborazione centrale (acoustic cryptanalysis attack);
- l’analisi termica della superficie del processore

(energia dissipata) per risalire al tipo di codice in esecuzione (thermal imaging attack/power attack);
- l’analisi dei fotoni emessi dal led di stato di un hard disk per ricostruire i dati in lettura e scrittura (optical side channel attack*);*
- l’analisi delle emissioni elettromagnetiche prodotte da dispositivi elettronici al fine di riscostruire, da queste, segnali e dati nascosti (le intercettazioni di tipo phreaking di Van Eck consentono di ricostruire le immagini sullo schermo di un computer tramite il rilevamento a distanza delle radiazioni emesse dai monitor).

Alla luce di quanto sopra esposto, se un utente malintenzionato riuscisse ad eseguire il proprio codice sul sistema, potrebbe per esempio sfruttare un timing attack attraverso il runtime di un’applicazione target osservando, a basso livello, i tempi di accesso alla memoria e di esecuzione, influenzandoli indirettamente forzando, ad esempio, lo stato cache ad un determinato valore e osservando la conseguente risposta dell’applicazione monitorata.

Possibili contromisure

È possibile utilizzare una serie di contromisure per prevenire potenziali tentativi di analisi di un canale laterale, basandosi essenzialmente su strategie che ostacolino le tecniche di correlazione (il rilascio di informazioni elettromagnetiche potrebbe, ad esempio, consentire di correlare uno specifico calcolo operazionale ad una determinata attività della CPU) attraverso una riduzione del rapporto segnale-rumore del canale secondario e/o una randomizzazione delle sequenze operazionali.

Anche se queste tipologie di attacchi, ormai note da tempo, non sembra abbiano avuto particolare risonanza rispetto ad altre forme di attacchi informatici a causa della loro

difficile applicazione (che richiede una presenza fisica in prossimità del target ed un certo monitoraggio), la facile reperibilità e disponibilità, oggigiorno, di dispositivi smart per la registrazione audio/video (IoT, smartphone, smartwatch ecc.) e l'infinita *varietà di canali secondari potenzialmente sfruttabili,* **per compromettere un sistema** attraverso fughe non intenzionali di dati, non rendono certamente trascurabile l'effettiva fattibilità.

https://www.key4biz.it/cybercrime-come-funziona-un-attacco-side-channel/325086/

Cybercrime, con il Covid-19 aumento di attacchi informatici. Il report di Europol

La pandemia globale di Covid-19 ha aumentato notevolmente gli attacchi informatici in tutto il mondo, e, nonostante l'impegno delle forze dell'ordine, il cybercrime non accenna a placarsi.

I risultati che emergono dalla settima edizione dell'*Internet Organised Crime Threat Assessment* (**IOCTA**) di **Europol**, l'agenzia anticrimine europea nata nel 1999, sono sconcertanti.

Secondo il report, uno studio accurato che fornisce

informazioni dettagliate sulle minacce emergenti e sugli sviluppi della sicurezza informatica, i criminali hanno rapidamente sfruttato la pandemia per attaccare gli utenti attraverso tecniche di phishing.

Inoltre, riferisce l'Europol, le truffe online e la diffusione di fake news sono diventate una strategia ideale per i criminali informatici che cercano di vendere articoli che, secondo loro, prevengono o cureranno il Covid-19.

Il report evidenzia come quest'anno il ransomware rimane la principale minaccia alla criminalità informatica, seguito dagli attacchi Phishing, dal materiale di sfruttamento sessuale dei minori e dall'exploit del deepweb. Durante questi mesi di pandemia infatti, il Deep Web è diventato terreno fertile per i criminali informatici, per fortuna, lo scorso 23 settembre, l'Europol è riuscita a dare un duro colpo alle organizzazioni criminali del deep web con l'operazione DisrupTor.

L'operazione DisrupTor

Lo scorso 23 settembre l'Europol ha dato al via l'operazione **DisrupTor**, che ha portato all'arresto di 179 criminali ritenuti responsabili di traffico di droga e armi nel Dark Web e al sequestro di 6,5 milioni di dollari sia in contanti che in valute virtuali di 500 chilogrammi di droghe, tra cui fentanil, ossicodone, idrocodone, metanfetamina, eroina, cocaina, ecstasy, MDMA e 64 armi da fuoco.

L'operazione **DisrupTor** era composta da una serie di operazioni congiunte separate ma complementari coordinate da **Europol** ed **Eurojust**, in collaborazione tra le forze dell'ordine e le autorità giudiziarie di Austria, Cipro, Germania, Paesi Bassi, Svezia, Australia, Canada, Regno Unito e Stati Uniti.

Per approfondire

https://www.key4biz.it/cybercrime-con-la-pandemia-aumenti-di-attacchi-informatici-lallarme-nel-nuovo-report-di-europol/324583/

Cybercrime, false email INPS diffondono il trojan Ursnif. L'avviso del Csirt

Il **CSIRT** Italia, il nuovo team per gestire la cyber-difesa nazionale italiana, ha individuato una nuova campagna di malspam che tenta di diffondere il trojan bancario **Ursnif** attraverso false email INPS, consegnando allegati Microsoft Office infetti a caselle di posta di utenze italiane.

Occhio alla false email INPS

Il messaggio, avvisa l'ente di gestione cyber, sembra provenire dall'Istituto Nazionale della Previdenza Sociale (INPS), ma è una truffa. L'oggetto della email è variabile tra "*Informazione Instituto Sociale*" o "Nazionale Previdenza Sociale" e anche layout e contenuti simulano una fase email INPS.

Lo scopo è quello di ingannare il destinatario e spingerlo ad aprire un file allegato .xls il cui nome inizia con "certificazione" seguito da "n_nn" (dove "n" rappresenta una combinazione numerica variabile). Di seguito un estratto della email:

Fonte: CSIRT Italia
Il documento, spiegano i ricercatori del Csirt, è armato con una macro e, come osservato nei recenti casi volti alla diffusione di malware, utilizza una tecnica di elusione elementare che consiste nel richiedere una password “2020” di apertura file che è fornita all’interno dello stesso messaggio.

Una volta aperto il file, alla vittima viene richiesto di abilitare la visualizzazione e la modifica del contenuto, informando lo stesso che il documento è stato scansionato ed è privo di virus.

Da un’analisi effettuata sulle richieste DNS dei domini riscontrati, è possibile confermare che i target principali di questa campagna sono utenti distribuiti su tutto il territorio italiano. Di seguito, a titolo esemplificativo, viene mostrato il grafico di distribuzione e timeline degli eventi delle richieste DNS per il dominio gstat.sloleaks[.]com:

Il trojan bancario Ursnif

Il trojan bancario **Ursnif**, scoperto nell’estate 2018 si è diffuso in questi anni attraverso diverse campagne malspam

sfruttando temi di vario genere ed ispirati a situazioni e/o eventi contemporanei. Questo tipo di malware finalizzato alla sottrazione di credenziali relative a servizi di home banking, continua purtroppo a rappresentare una reale minaccia che riappare periodicamente sfruttando sempre strategie diverse.

Non a caso secondo il recente rapporto di Check Point Research (Global Threat Index 05/2020) questo malware è entrato per la prima volta nella top 10 delle minacce rilevate, posizionandosi al quinto posto a livello globale.

Nello specifico in Italia, nel mese di maggio Ursnif si è piazzato al primo posto registrando un impatto sulle organizzazioni di oltre il 14% (contro una media mondiale del 2%).

Azioni consigliate secondo il CSIRT

Per far fronte a questa tipologia di attacchi, il Csirt consiglia di verificare attentamente le email ricevute seguendo le seguenti misure:

- limitare le funzionalità delle macro che attivano connessioni verso internet;
- diffidare dalle richieste di inserimento password in allegati sospetti;
- valutare la verifica e l'implementazione sui propri apparati di sicurezza dei seguenti Indicatori di Compromissione (IoC)

Cybercrime, false email INPS diffondono il trojan Ursnif. L'avviso del Csirt

CyberChallenge.IT, l’Università di Pisa vince la gara nazionale degli hacker etici

L’**Università di Pisa** è la vincitrice della quarta edizione di **CyberChallenge.IT**, la gara nazionale degli hacker etici italiani, organizzata ogni anno dal Laboratorio Nazionale di Cybersecurity del **CINI** (Consorzio Interuniversitario Nazionale per l’Informatica).

L’evento, per la prima volta interamente online, ha coinvolto 560 ragazzi tra i 16 e i 23 anni, per un totale di 28 squadre, rappresentate da 26 università, il Centro di Competenza Cybersecurity Toscano e il Comando per la Formazione e Scuola di Applicazione dell’Esercito di Torino. A conquistare il primo gradino del podio, per questa edizione, è stata l’Università di Pisa, con il **Politecnico di Milano** al secondo posto e l’**Università degli Studi di Verona** terza classificata.

CyberChallenge.IT e il Cyber range Paideusis

I team si sono confrontati in una complessa gara di tipo *Capture the flag* (Ctf), una sorta di ruba bandiera virtuale, nella quale ciascuna squadra è stata chiamata ad attaccare le infrastrutture informatiche degli avversari, proteggendo al contempo la propria, e impedendo ad altri di prenderne il controllo. Uno dei campi di battaglia, creato apposta per l’occasione, è stato il nuovo cyber range *Paideusis*: un’infrastruttura permanente, fisicamente ospitata a Torino

dalla **Fondazione Links,** che l'ha realizzata insieme al Laboratorio Nazionale di Cybersecurity e con la collaborazione tecnica dell'azienda canavese **Tiesse**.

"In qualità di fornitore il nostro contributo è stato quello di fornire le piattaforme hardware di rete -router- per Paideusis", ha dichiarato **Vincenzo Luciano Lucrezia**, CTO di Tiesse S.p.A. *"Crediamo infatti ,* aggiunge il CTO, *"che il sostegno concreto ad iniziative di questo genere, eccellenze a livello Europeo, siano fondamentali per il trasferimento di conoscenze, per lo sviluppo di innovazione e che offrano stimoli a tutte le parti coinvolte giovani compresi".*

Tutta contenuta in una sola stanza, *Paideusis* consiste in un ambiente fisico accessibile in remoto nel quale interagiscono tra loro i modem di ciascun team.

"Vedere la gara nel vivo, pur da remoto, è stata la più grande soddisfazione dopo mesi di lavoro nel quale abbiamo fatto i conti, come tutti, con una pandemia globale", ha commentato **Paolo Prinetto**, direttore del Laboratorio Nazionale di Cybersecurity. *"Questa è la più significativa dimostrazione di come, pur con 560 ragazzi e ben 28 istituzioni coinvolte, ogni problema può diventare opportunità, quando la motivazione è forte e rivolta alla cultura della sicurezza e del progresso tecnologico. Ci sono tutte le basi per crescere ancora e – speriamo – per poter realizzare la prossima CyberChallenge.IT in presenza"*.

Il TeamItaly

Il prossimo passo nelle attività del Laboratorio Nazionale di Cybersecurity sarà la convocazione dei giovani che si sono maggiormente distinti durante le gare per l'ingresso nel TeamItaly: la nazionale italiana di esperti di sicurezza informatica che ogni anno rappresenta l'eccellenza del Paese nelle competizioni nazionali.

Il prossimo appuntamento sarà a novembre, con un'amichevole a livello europeo organizzata dall'Agenzia europea per la sicurezza delle reti e dell'informazione (**ENISA**), che sostituisce il campionato europeo (European Cybersecurity Challenge – Ecsc), rimandato a causa del Covid-19. Resta quindi – d'ufficio – sul podio europeo anche la nazionale italiana, che a Ecsc19 aveva conquistato il secondo posto.

Ottobre è il mese europeo della cybersecurity

Il 1° ottobre ha preso il via l'ottava edizione del mese europeo della cybersecurity, l'iniziativa dell'Unione Europea che riunisce i suoi Stati membri e i cittadini europei per prevenire e contrastare le minacce informatiche.

Per l'intero mese nel vecchio continente si svolgeranno centinaia di attività, coordinate dall'ENISA. Conferenze, seminari, sessioni di formazione, presentazioni generali, webinar e campagne online, mirate a sensibilizzare i cittadini sulla cybersecurity ed a fornire informazioni aggiornate sulla sicurezza digitale attraverso la formazione e la condivisione delle migliori pratiche.

https://www.key4biz.it/cyberchallenge-it-luniversita-di-pisa-vince-la-gara-nazionale-degli-hacker-etici/324122/