Cybercrime, la botnet KashmirBlack prende di mira le piattaforme CMS. Come difendersi

Un team di ricercatori statunitense ha fornito dei report dettagliati riguardo a una nuova botnet denominata **KashmirBlack** che, sulla base dei numerosi indizi trovati, si ritiene sia opera di *"Exect1337"* un membro del gruppo hacker indonesiano **PhantomGhost**.

Tale botnet utilizzata molto probabilmente per attività di cripto mining, spam e *defacement* per diffondere ed espandere il proprio raggio di azione (arruolando nuovi bot) si propaga attraverso exploit di note piattaforme CMS (**WordPress, Joomla!, PrestaShop, Magento, Drupal, Vbulletin, OsCommerence, OpenCart e Yeager**) utilizzando, inoltre, i servizi basati su cloud **Github, Pastebin e Dropbox** come mezzo per celare e gestire la botnet stessa.

KashmirBlack: modalità di funzionamento

I ricercatori hanno individuato, durante la propria attività di telemetria (avvenuta tra novembre 2019 e fine maggio 2020, seppur la bonet risulti tutt'oggi ancora operativa) circa 700.000 tentativi di attacchi giornalieri con ben 285 bot in azione, ma il numero potrebbe molto probabilmente essere ancor più consistente anche in considerazione dell'evoluzione osservata.

La botnet KashimirBlack inizialmente di medio volume con capacità standard si è presto trasformata in una ben progettata e complessa infrastruttura, ad oggi, costituita da un server C2 con più di 60 server surrogati come parte integrante del proprio impianto.

Il server di comando e controllo (C2) capace di gestire centinaia di bot svolge principalmente tre compiti:

1. fornisce uno script Perl per l'infezione del server vittima;
2. riceve dai bot i rapporti sui risultati;
3. fornisce ai bot le istruzioni di attacco.

I bot, invece, possono trovarsi secondo necessità in due stati differenti:

- Attivo. I "spreading bot" possono effettuare operazioni tese ad estendere la dimensione della botnet, comunicando con il server C2 per ricevere indicazioni sui nuovi target, eseguire attacchi brute force e installare backdoor come teste di ponte;
- Standby. I "pending bot" restano in attesa di cambiare stato, ascoltando periodicamente il canale di comunicazione instaurato con il server C2.

Vulnerabilità sfruttate per la diffusione

Secondo quanto riportato dallo studio, l'attività monitorata starebbe ancora generando diversi attacchi contro migliaia di vittime sparse in tutte il mondo, diffondendosi grazie alla compromissione di siti web in esecuzione su piattaforme CMS non aggiornate e potenzialmente vulnerabili anche a certi exploit su plugin, librerie e componenti interne:

- PHPUnit Remote Code Execution – CVE-2017-9841
- jQuery file upload vulnerability – CVE-2018-9206

- ELFinder Command Injection – CVE-2019-9194
- Joomla! remote file upload vulnerability
- Magento Local File Inclusion – CVE-2015-2067
- Magento Webforms Upload Vulnerability
- CMS Plupload Arbitrary File Upload
- Yeager CMS vulnerability – CVE-2015-7571
- WordPress TimThumb RFI Vulnerability – CVE-2011-4106
- Uploadify RCE vulnerability
- vBulletin Widget RCE – CVE-2019-16759
- WordPress install.php RCE
- WordPress xmlrpc.php Login Brute-Force attack
- WordPress multiple Plugins RCE
- WordPress multiple Themes RCE
- Webdav file upload vulnerability

KashmirBlack: come difendersi

Per impedire e rilevare possibili tentativi di attacco i ricercatori hanno fornito diversi consigli e dettagli tecnici specifici.

In particolare, ciò che raccomandano agli amministratori dei siti web è di assicurare innanzitutto:

- l'aggiornamento periodico e la corretta configurazione non solo dei CMS ma anche degli eventuali moduli extra di terze parti;
- un'adeguata gestione delle password per contrastare gli attacchi brute force;
- una protezione ulteriore dei propri siti, tramite l'adozione di firewall WAF utili per le applicazioni Web;
- un controllo preventivo rimuovendo processi sospetti, plugin e temi inutilizzati oltre che negare l'accesso a file e directory fondamentali di sistema e configurazione PHP.

Cybercrime, la botnet KashmirBlack prende di mira le

piattaforme CMS. Come difendersi

Ransomware e Covid, l'FBI avverte gli ospedali: 'Alto rischio di attacchi, si rischia il blocco delle strutture'. Il report

I criminal hacker stanno prendendo di mira il settore sanitario utilizzando virus malevoli e attacchi *ransomware*, c'è il rischio di una *"minaccia informatica imminente"*.

L'annuncio arriva direttamente dall'FBI e altre due agenzie governative nel report "***Ransomware Activity Targeting the Healthcare and Public Health Sector***" disponibile qui.

Gli enti di sicurezza degli Stati Uniti affermano infatti di avere *"informazioni credibili"* e lanciano l'allarme per ospedali e operatori sanitari già alle prese con una pandemia che finora ha fatto più di 227mila vittime nel Paese.

La minaccia arriva mentre gli ospedali statunitensi sono alle prese con un numero crescente di casi di coronavirus. Per questo motivo le agenzie federali hanno esortato gli operatori sanitari statunitensi a prendere *"precauzioni tempestive e ragionevoli"* per proteggere le loro reti.

Le agenzie consigliano inoltre di cambiare regolarmente le password e di utilizzare l'autenticazione a più fattori.

Hanno incoraggiato gli operatori sanitari a proteggere i loro sistemi operativi e i software il prima possibile e a condurre regolarmente scansioni antivirus e antimalware.

L'FBI al personale sanitario: difendetevi dai Ransomware

Il ransomware è un tipo di software dannoso utilizzato dai criminali informatici per crittografare i file degli utenti fino al pagamento di un riscatto. Le istituzioni sanitarie sono state vittime frequenti di ransomware per diversi anni negli Stati Uniti e nel mondo.

Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

- sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);
- contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli

Il mese scorso, un sospetto attacco ransomware ha interrotto l'assistenza ai pazienti in un'ampia catena di ospedali e

cliniche che operano negli Stati Uniti e in Gran Bretagna. In Germania, un attacco ransomware alla struttura informatica di un pronto soccorso, che ha portato all'interruzione dei sistemi e alla sospensione delle attività ambulatoriali e di emergenza, ha portato al decesso di una donna che non ha potuto ricevere le cure sanitarie urgenti di cui necessitava, ritardate a causa del trasferimento in altra struttura.

Per approfondire

Scarica il report in esclusiva ***Ransomware Activity Targeting the Healthcare and Public Health Sector*** qui

https://www.key4biz.it/ransomware-e-covid-lfbi-avverte-gli-ospedali-alto-rischio-di-attacchi-si-rischia-il-blocco-delle-strutture-il-report/328250/

La Cybersecurity ha a disposizione le tecnologie adeguate? Scarica il Report

Un'organizzazione indipendente che riunisce esperti del settore per discutere su come migliorare la cybersecurity, **Debate Security**, ha pubblicato una ricerca sulle prestazioni inefficaci del mercato della sicurezza informatica.

Sulla base di oltre 100 interviste con leader aziendali e grandi imprese, insieme a fornitori, organizzazioni di valutazione, agenzie governative, associazioni di settore e

regolatori, la ricerca di Debate Security fa luce sul perché i fornitori di tecnologia non sono incentivati a fornire prodotti più efficaci a ridurre il rischio cibernetico.

L’inefficacia della cybersecurity? Questioni economiche e non tecnologiche

Il report Cybersecurity Technology Efficacy: Is Cybersecurity The New “Market for Lemons” ?, sostiene l’opinione che i problemi di efficacia nel mercato della cybersecurity siano principalmente dovuti a questioni economiche, non tecnologiche. La ricerca affronta tre temi chiave e alla fine arriva a un consenso su come affrontare un nuovo modello:

- **La tecnologia non è così efficace come dovrebbe essere**

Il 90% dei partecipanti ha riferito che la tecnologia di sicurezza informatica non è efficace come dovrebbe essere quando si tratta di proteggere le organizzazioni dal rischio informatico.

- **Il problema di fondo è l’economia, non la tecnologia**

Per la ricerca il 92% dei partecipanti ha riferito che c’è una rottura nel rapporto di mercato tra acquirenti e fornitori, con molti che vedono asimmetrie informative profonde. Al di fuori del Governo, oggi pochi acquirenti utilizzano una valutazione dell’efficacia della sicurezza informatica dettagliata e indipendente come parte del loro processo di approvvigionamento di sicurezza informatica e nemmeno le organizzazioni più grandi hanno dichiarato di avere le risorse per condurre da sole tutte le valutazioni. Di conseguenza, i fornitori sono incentivati □□a concentrarsi su altre caratteristiche del prodotto e sul marketing, riducendo le priorità dell’efficacia della tecnologia di sicurezza informatica, uno dei numerosi segni classici di un “mercato

dei limoni”.

- **A meno che gli acquirenti non richiedano una maggiore efficacia, la regolamentazione potrebbe essere l’unico modo per affrontare il problema.**

Il 70% degli intervistati ritiene che una valutazione indipendente e trasparente della tecnologia aiuterebbe a risolvere il crollo del mercato. Stabilire standard sulla valutazione della tecnologia piuttosto che sulla tecnologia stessa potrebbe impedire il soffocamento dell’innovazione.

Scarica il report

Clicca qui per scaricare il report

https://www.key4biz.it/la-cybersecurity-ha-a-disposizione-le-tecnologie-adeguate-scarica-il-report/327972/

Luxottica, pubblicati sul dark web i dati rubati dal recente attacco hacker

Per molti, la reazione di **Luxottica** all’attacco hacker subito di recente, era stata da manuale. Ma secondo **Odisseus**, esperto indipendente di sicurezza informatica, non sembra affatto così.

Attraverso un tweet, Odisseus fa sapere che il gruppo criminale **Nefilim** ha pubblicato sul **dark web 2 GB** di dati che sembrano provenire dall’hacking dello scorso 20 settembre ai danni della multinazionale.

> *The #Nefilim hacker group published #Luxottica's files after the #ransomware attack.*
>
> *Two file lists and 2 GB of data stored in the #darkweb:*
>
> *— LUXOTICA_Human_Res_part1_filelist_part1.txt*
> *— LUXOTICA_Finance_part1_filelist.txt*
> *pic.twitter.com/i16PHl9Tbh*
>
> *— Odisseus (@_odisseus) October 20, 2020*

Nel tweet di **Odisseus** ci sono due screenshot relativi a due file. Uno fa riferimento alle risorse umane, l'altro al dipartimento finanziario.

Non sappiamo nel dettaglio il contenuto dei due file, ma c'è il concreto rischio che siano incluse informazioni personali sui dipendenti e dati sensibili di carattere finanziario.

Attacco ransomware a Luxottica, i dettagli

Su key4biz siamo stati tra i primi a riportare la notizia dell'attacco informatico alla società guidata da **Leonardo Del Vecchio**. L'hack, che ha riguardato in particolare le sedi Luxottica di Agordo e Sedico, in provincia di Belluno, ha provocato il blocco della produzione e la sospensione dei turni degli operai.

Se in un primo momento si è parlato di gravi problemi informatici, come rete fuori uso, il blocco dei computer e l'impossibilità ad eseguire qualsiasi operazione, sarebbe poi stato confermato un attacco ransomware. Per la società è stato

un tentativo di violare i sistemi informatici che non avrebbe avuto esito positivo grazie all'attivazione dei meccanismi di difesa.

Il rischio di una multa

Secondo quanto riportato dal sito *Bleeping Computer* i criminali informatici avrebbero sfruttato una vulnerabilità nota dall'inizio dell'anno nei prodotti VPN di Citrix for Cyber-Attacks, con la quale ottenere credenziali per l'accesso e la diffusione all'interno di una rete. La stessa vulnerabilità che avrebbe consentito l'attacco ransomware ad un ospedale tedesco pochi giorni prima, dalle conseguenze ben peggiori.

Se il data breach però dovesse risultare vero, diventerebbe un grave danno all'immagine della multinazionale. Inoltre l'azienda potrà ricevere una sanzione per violazione della privacy in materia di GDPR da parte dell'Autorità Garante.

https://www.key4biz.it/luxottica-pubblicati-sul-dark-web-i-dati-rubati-dal-recente-attacco-hacker/327173/

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/

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/

Ue, al via il CyberSecurityMonth. Vestager: “La cybersecurity riguarda tutti noi”

“Prima di cliccare, pensaci”. E’ questo il claim dell’ottava edizione del mese europeo della cybersecurity, che riunisce l’Unione europea, i suoi Stati membri e i cittadini europei per prevenire e contrastare le minacce informatiche.

L’obiettivo principale della campagna di quest’anno, che inizia oggi, 1º ottobre, è garantire che i cittadini siano consapevoli dei rischi online e dispongano degli strumenti necessari per diventare utenti di tecnologie più resilienti e più sicuri.

“Visto che la nostra vita quotidiana e le nostre economie stanno diventando sempre più dipendenti dalle soluzioni digitali, dobbiamo renderci conto che la sicurezza informatica riguarda tutti noi”, ha dichiarato **Margrethe Vestager**, Vicepresidente della Commissione Europea titolare per la Concorrenza. *“È importante promuovere una cultura della sicurezza all’avanguardia nei settori vitali della nostra economia e della nostra società.”*

Margaritis Schinas, Vicepresidente responsabile per la Promozione dello stile di vita europeo, ha aggiunto:*”Il mese europeo della cybersecurity mira a sensibilizzare l’opinione pubblica sulla sicurezza informatica e a renderci consapevoli*

delle minacce informatiche. Ci rammenta che possiamo facilmente rafforzare la nostra cibersicurezza adottando buone abitudini digitali. E' essenziale per il nostro stile di vita europeo."

Thierry Breton, Commissario per il Mercato interno, ha concluso: "*Come lo spazio terrestre, marittimo o aereo, lo spazio dell'informazione digitale presenta talvolta lacune in materia di sicurezza, lacune che vanno colmate. La nostra ambizione è fornire ai cittadini dell'UE lo spazio dell'informazione più sicuro al mondo. A tal scopo ci affideremo soprattutto all'istruzione. È questo l'obiettivo del mese europeo della cybersecurity 2020, che lanceremo domani per sensibilizzare i cittadini sulle competenze in materia di sicurezza online e cibersicurezza, fondamentali per il futuro.*"

Ottobre mese europeo della Cybersecurity

Per l'intero mese in tutta Europa si svolgeranno centinaia di attività, coordinate dall'Agenzia europea per la cibersicurezza (ENISA).

Si terranno 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.

L'Italia e la sicurezza informatica

Nelle ultime settimane in Italia si è visto un incremento massiccio di attacchi informatici rivoli ad Istituzioni ed imprese. Il più grave, per le conseguenze avute, rimane l'attacco al **Gruppo Carraro**, azienda italiana leader internazionale nel comparto delle macchine agricole.

L’azienda, a causa dell’attacco subito che ha paralizzato i sistemi informatici di tutta l’attività del gruppo, da quella amministrativa a quella produttiva, altamente automatizzata da robot, ha dovuto mettere settecento dipendenti in cassa integrazione tra gli stabilimenti di Campodarsego e quelli della divisione Agritalia di Rovigo in attesa del ripristino dei sistemi.

L’attacco informatico era avvenuto a distanza di pochi giorni da quello analogo che aveva colpito **Luxottica**, la più grande produttrice mondiale di montature per occhiali da vista e da sole

https://www.key4biz.it/ottobre-e-il-mese-europeo-della-cybersecurity-vestager-la-sicurezza-informatica-riguarda-tutti-noi/323683/