La Merkel vuole che l'Ue sanzioni la Russia per l'attacco hacker al Bundestag del 2015

Il governo tedesco ha proposto ufficialmente che l'Unione europea imponga sanzioni contro la Russia, Paese responsabile dell'hack al **Bundestag** avvenuto nel 2015.

Se concordato, questo potrebbe essere il primo utilizzo del sistema di sanzioni informatiche dell'UE adottato nel 2017.

Il governo tedesco ritiene che l'intelligence russa sia alla base dell'attacco hacker al parlamento tedesco avvenuto cinque anni fa.

Nell'hack circa 16 gigabyte di dati, documenti ed e-mail sono stati sottratti dalla rete IT del Bundestag, tra cui migliaia di e-mail dall'ufficio Bundestag della cancelliera tedesca **Angela Merkel.**

L'attacco è considerato il più grande cyber hacking mai realizzato contro il Bundestag.

L'attacco hacker al Bundestag nel 2015

A maggio, parlando al Bundestag, la cancelliera ha riferito che l'inchiesta della Procura generale ha rilevato "*prove schiaccianti*" del coinvolgimento russo nell'attacco informatico, dichiarando che la Germania "*si riserva il diritto di prendere misure contro la Russia*".

Secondo varie ricostruzioni di stampa, gli investigatori tedeschi ritengono il **Gru**, l'intelligence militare russa, responsabile dell'attacco informatico. La Procura generale tedesca avrebbe ottenuto un mandato di arresto internazionale nei confronti di un giovane hacker russo, **Dmitry Badin**, "fortemente sospettato di essere responsabile" dell'attacco.

Chi è Dmitry Badin

Badin ha solo 30 anni ma è già un'autorità nel mondo hacker. E' un membro del gruppo **APT28**, un gruppo paramilitare di hacker ritenuti collegati al GRU.

L'agente, secondo un'indagine di **Bellingcat**, il più famoso team di giornalisti investigativi al mondo, era già nella lista di ricercati dell'Fbi per aver preso parte a diverse operazioni della famigerata unità di spie russe.

Fra queste, l'hackeraggio dell'organizzazione anti-doping Wada, e soprattutto quello del Comitato nazionale democratico e delle elezioni presidenziali del 2016 finite nelle carte del Russiagate.

https://www.key4biz.it/la-merkel-vuole-che-lue-sanzioni-la-russia-per-lattacco-hacker-al-bundestag-del-2015/314120/

Guerra cyber Usa-Russia, Trump conferma attacco all'IRA

Donald Trump ha confermato per la prima volta che gli Usa hanno condotto un cyber attacco segreto nel 2018 contro la

Internet Research Agency (IRA) russa, una società di troll accusata di aver interferito nelle presidenziali Usa del 2016 e in quelle di midterm del 2018.

Secondo quanto riporta il Washington Post, il tycoon ha svelato l'attacco in una intervista a **Marc Thiessen**, giornalista del quotidiano.

Trump conferma attacco all'Internet Research Agency

Il Presidente durante l'intervista ha affermato che gli USA hanno "fermato le interferenze Russe" senza però rilasciare nessun dettaglio dell'operazione.

La conferma dell'attacco informatico costituisce un radicale cambio di atteggiamento per Trump, che in passato ha più volte negato che vi siano state interferenze da Mosca durante le elezioni presidenziali del 2016.

La Russia cosa farà?

Con tutta probabilità non vi saranno interventi dalla Russia, considerando come il Cremlino non abbia mai confermato i legati tra le istituzioni del Paese e le attività della **Internet Research Agency**, ufficialmente un'azienda privata con sede a **San Pietroburgo**.

Washington ha già messo in campo una task force in vista della chiamata alle urne fissata per questo autunno, quando il 3 novembre 2020 si voterà per le elezioni presidenziali, così da evitare che possa verificarsi di nuovo quanto accaduto quattro anni fa.

Il cyber command degli Stati Uniti

Gli Usa hanno sferrato l'attacco grazie al Cyber Command degli Stati Uniti, uno degli undici comandi unificati del Dipartimento della Difesa degli Stati Uniti.

Il Cyber Command, istituito nel 2010 dall'amministrazione **Obama**, ha attualmente la responsabilità delle operazioni nel cyberspace e la protezione delle reti degli apparati militari statunitensi e opera all'interno dell'United States Strategic Command, che si occupa delle operazioni spaziali, della sicurezza delle informazioni, della dissuasione strategica nucleare e altri compiti simili.

https://www.key4biz.it/guerra-cyber-usa-russia-trump-conferma-attacco-allira/314001/

Zoom, scoperta vulnerabilità su Windows 7

Un bug nel software di videoconferenza **Zoom** potrebbe consentire ad un criminal hacker di comandare in remoto un Pc che detiene vecchie versioni del sistema operativo **Microsoft Windows.**

La nuova vulnerabilità "zero-day", hanno dichiarato i ricercatori di sicurezza **ACROS Security,** la società di sicurezza informatica che ha evidenziato il problema, a Cyberscoop, *si applica al software Zoom in esecuzione su Windows 7 o anche sistemi operativi precedenti che al momento sono fuori uso.*

Al momento non sono stati resi noti ulteriori dettagli riguardo il bug. Inoltre non è ancora disponibile una patch che risolva il problema di sicurezza.

Molti utenti utilizzano ancora Windows 7

La buona notizia è che Microsoft ha tentato di eliminare gradualmente il supporto tecnico per Windows 7 nel tentativo di incoraggiare gli utenti a passare a sistemi operativi più sicuri. Ma Windows 7 è ancora ampiamente utilizzato e molte aziende fanno fatica a spostare sui propri computer il più recente software Windows.

"*Zoom prende sul serio tutte le segnalazioni di potenziali vulnerabilità della sicurezza*", ha dichiarato un portavoce di Zoom in una nota, confermando quindi il problema di sicurezza. "*Ieri abbiamo ricevuto una segnalazione di un problema che ha avuto un impatto sugli utenti con Windows 7 e versioni precedenti. Abbiamo confermato questo problema e stiamo attualmente lavorando su una patch per risolverlo rapidamente.* "

Zoom e le falle di sicurezza

Si parla spesso del ruolo della sicurezza su Zoom, piattaforma di videochiamate la cui popolarità è aumentata vertiginosamente in tutto il mondo durante la pandemia di Coronavirus. Il servizo è passato da 10 milioni di utenti al giorno nel mondo, registrati a dicembre 2019 prima dell'emergenza sanitaria, a 200 milioni nel mese di marzo.

Allora come usare Zoom in modo più sicuro? Recentemente su Key4biz abbiamo diffuso una miniguida su come usare al meglio

la piattaforma. Ecco 6 consigli:

- Non rendere pubblico il link delle riunioni o lezioni online. Zoom offre due opzioni per rendere privata una riunione: richiedere una password della riunione o utilizzare la funzione di sala d’attesa e controllare così chi può partecipare.
- Non diffondere il proprio Personal Meeting ID (**PMI**) e usarlo per ogni riunione di Zoom, perché se qualcuno entra in possesso del link alla vostra sala riunioni personale, può entrare e disturbare quando vuole. Un approccio migliore è quello di generare ID unici con relative password per le vostre riunioni.
- Non condividere il collegamento a una teleconferenza o a una lezione in un post sui social network.
- Fornisci il link della videocall direttamente a persone specifiche.
- Gestisci le opzioni di condivisione dello schermo. In Zoom, modifica la condivisione dello schermo in “Solo ospiti”.
- Assicurarsi che i partecipanti stiano utilizzando la versione aggiornata di Zoom. Nella versione di gennaio 2020 ha aggiunto le password per impostazione predefinita per le riunioni e ha disabilitato la possibilità di cercare casualmente le riunioni per partecipare.

Zoom, scoperta vulnerabilità su Windows 7

Joker, come funziona il malware Android che elude la sicurezza di Google

Apparso in natura per la prima volta nel 2017, il **malware Joker**, ovvero uno spyware sofisticato concepito per commettere frodi informatiche è stato nuovamente individuato dai ricercatori di **Check Point Research** in nuova variante.

Il malware Joker

Questa volta, continuando a eludere i sistemi di protezione dello Store di **Google**, ha agito per fare attivare servizi a pagamento alle vittime ignare colpite, celandosi in modo subdolo in ben 11 app.

Figura: Una delle app/Joker rilevate su Google Play Store da Chek Point Research

La tecnica di offuscamento

Nel tentativo di offuscare l'impronta digitale di Joker, i criminal hacker hanno nascosto il caricamento dinamico del file .dex, file di inizializzazione previsto dai sistemi Android, pur garantendone il download attraverso una strategia simile a quella ben nota agli sviluppatori di malware per PC Windows.

In questa nuova veste, infatti, il codice dannoso del malware,

noto anche con il nome di Bread, si nascondeva, come file “dex” sotto forma di stringhe codificate in Base64, all’interno del cosiddetto file di progetto xml “AndroidManifest” che ogni app deve contenere nella sua directory principale, per fornire al sistema ospitante determinate informazioni essenziali per una corretta esecuzione del codice.

Con questo escamotage i criminal hacker sono riusciti, così, ad evitare l’accesso ad un server C2 per inviare comandi ai sistemi compromessi e scaricare definitivamente il payload, azioni che sarebbero state di sicuro captate dalle ultime routine di sicurezza adottate da Google.

La catena d’infezione

Come spiegato dagli stessi analisti, gli sviluppatori criminali in questa versione del malware hanno implementato un processo d’infezione suddiviso in tre fasi, sempre allo scopo di migliorarne l’offuscamento e l’invisibilità, arginando così scrupolosamente i controlli di sicurezza che il Play Protect Google aggiorna periodicamente:

1. **creazione del payload**: il payload viene inserito nel file “Android Manifest”;
2. **attesa per il caricamento del payload**: durante tutto il tempo necessario per il processo di valutazione dell’app, Joker resta dormiente per bypassare le protezioni di Google Play Store;
3. **diffusione del payload**: cessato il periodo di valutazione e dopo l’avvenuta approvazione dell’app, Joker si attiva e il payload viene caricato sul dispositivo dell’ignara vittima.

Come difendersi

In questi ultimi anni, il malware Joker con le sue varianti,

come confermato dalla stessa Google, è riuscito, tramite diverse tecniche di cloaking, a mascherare il proprio contenuto malevolo celandosi in applicazioni apparentemente legittime, diventando, di fatto, una delle più gravi minacce persistenti del suo genere.

Alla luce di quanto detto, poiché non si può escludere che Joker torni a far danno sotto altre mentite spoglie e qualora si dovesse sospettare di avere installato una di queste app sul proprio dispositivo, è di fondamentale importanza:

- disinstallare l'app presumibilmente infetta;
- controllare le liste movimenti di carte di pagamento e del credito residuo smartphone presso il proprio gestore telefonico, controllando che non siano stati attivati eventuali abbonamenti anomali;
- prevenire future infezioni proteggendo il proprio smartphone con una soluzione di protezione adeguata.

I ricercatori di sicurezza hanno ovviamente divulgato la scoperta in modo responsabile a Google e già dallo scorso 30 aprile le app segnalate risultano rimosse dal Play Store. Di seguito si riportano gli IoC dei *package* resi pubblici.

https://www.key4biz.it/joker-come-funziona-il-malware-android-che-elude-la-sicurezza-di-google/313726/

Cyber crime, frodi

informatiche da 20 milioni di euro l’anno tra Italia e Romania

È ancora in corso l’operazione “***Last Chain***” della **Polizia Postale** italiana, in collaborazione con **Eurojust**, **Europol** e **Polizia rumena**, con arresti e sequestri tra Italia e Romania, e l’obiettivo di smantellare un’organizzazione cyber criminale tra le più grandi d’Europa.

Il giro d’affari è stato quantificato in più di 20 milioni di euro l’anno. Una cifra considerevole, frutto di truffe e frodi informatiche compiute dal gruppo criminale in tutta Europa.

C’era un primo livello operativo di cyber crime in Romania, che aveva il compito di sottrarre risorse finanziarie ad ignari utenti di rete, prelevando i soldi direttamente dai conti correnti.

Un secondo livello invece tutto italiano, che doveva gestire i proventi criminali tramite attività di riciclaggio e conti correnti intestati a prestanome, da cui poi i soldi venivano prelevati e trasportati fisicamente in Romania.

Le indagini e gli arresti sono stati coordinati dalla Procura di Genova, mentre sequestri di beni immobili e di denaro contante sono in corso nei due Paesi, tra ville, appartamenti, automobili e negozi.

Secondo l’ultimo Rapporto Clusit 2020, le attività di cyber crime sono cresciute costantemente nell’ultimo anno: rispetto al 2018 del +12,3% e del +162% rispetto al 2014.

Un cyber crimine che continua a sfruttare, attraverso il

phishing e anche l’impiego di servizi già pronti, sempre più efficaci, semplici da utilizzare e facilmente reperibili a basso costo sul dark web, la scarsa consapevolezza delle persone per indurle a eseguire azioni potenzialmente pericolose, carpendo dati, informazioni sensibili e altro ancora.

Una delle principali cause di violazioni, phishing e incidenti di varia natura, è infatti la vulnerabilità dell’utente finale correlata alla sua debolezza nel riconoscere e fronteggiare una possibile trappola informatica.

> *Cyber crime, frodi informatiche da 20 milioni di euro l’anno tra Italia e Romania*

Giovanni Reccia (GdF) ‘Tre anni vissuti intensamente a combattere il crimine informatico’

Si è chiuso oggi con una mega operazione antifrode relativa a servizi mobili a valore aggiunto non richiesti (VAS) il triennio del colonnello **Giovanni Reccia**, comandante del Nucleo Speciale Privacy e Frodi Tecnologiche (GdF). Un triennio denso di operazioni chiuse con successo, tre anni vissuti intensamente. Sono almeno una ventina quelle di maggior rilievo, che vanno dallo smantellamento di una rete di falsi broker assicurativi, al blocco di piattaforme abusive di trading online, al sequestro di 28 siti web e canali Telegram

che pubblicavano illegalmente giornali online. E ancora, al sequestro di falsi farmaci anti coronavirus, all'arresto di tre amministratori di black market nel dark web (la famosa operazione Berlusconi Market), alla disattivazione di un network internazionale di contenuti televisivi pirata, passando per truffe informatiche di ogni tipo, al sequestro di prodotti contraffatti sui social network, a quello di prodotti da fumo venduti illegalmente in rete, al riciclaggio di denaro nel dark web. Un campionario vastissimo di crimini informatici. Ne abbiamo parlato con il comandante **Giovanni Reccia**, per fare un bilancio di tre anni vissuti in prima linea contro il crimine informatico.

Key4biz. ***Comandante, come si è chiusa l'ultima operazione di smantellamento dei servizi VAS?***

Giovanni Reccia. Si è chiusa con 11 indagati e 12 milioni di euro già sottoposti a sequestro preventivo dei Csp che producono i servizi aggiuntivi per le compagnie telefoniche che erogano i servizi. Sono migliaia gli utenti a cui sono stati accreditati importi non dovuti per attivazioni indebite dei cosiddetti Servizi a valore aggiunto (VAS) sul proprio dispositivo mobile. Questi servizi devono normalmente essere autorizzati dall'utente intestatario del numero telefonico, invece con un meccanismo particolare sono automaticamente rilasciati dal servizio stesso, in maniera inconsapevole dall'utente.

Key4biz. ***Si tratta di una pratica fraudolenta diffusa?***

Giovanni Reccia. Sì. E' un business illecito da milioni di euro con opportunità di guadagno anche mediante le attivazioni dei servizi VAS sulle connessioni mobili usate tra macchine per lo scambio di dati (le cosiddette machine to machine, M2M) senza alcun consenso da parte di utenti. L'**AGCOM** è stata

compiutamente informata. Vi è l'impegno di tutti per interrompere, definitivamente, tale illecito fenomeno. La Procura di Milano ha contestato l'accesso abusivo nel creare un meccanismo inconsapevole di pagamento da parte dell'utente e la frode informatica.

Key4biz. ***Si tratta di una frode che riscontrate spesso?***

Giovanni Reccia. Il problema vero è che si tratta di un meccanismo sistematizzato che va risolto.Per questo la Procura ha inviato una missiva all'Agcom evidenziando che i servizi VAS a valore aggiunto devono essere staccati e venduti separatamente dalla scheda telefonica.

Key4biz. ***Si chiude con questa operazione il suo triennio al comando Nucleo Speciale Privacy e Frodi Tecnologiche (GdF). Qual è il suo bilancio personale?***

Giovanni Reccia. Tre anni vissuti intensamente, un periodo ricchissimo di operazioni ed investigazioni mai fatte prima.

Key4biz. ***Che tipo di operazioni avete svolto in questo triennio?***

Giovanni Reccia. Abbiamo spaziato da tutte le parti: dal dark web – con l'operazione Berlusconi Market, con la Procura di Brescia, siamo stati gli unici al mondo insieme all'FBI ad aver chiuso un black market – alla contraffazione, alla pirateria digitale, alle intercettazioni abusive. Siamo stati gli unici a fare un'operazione internazionale antipirateria digitale, con l'operazione Black IP Tv con la Procura di Napoli.

Poi abbiamo fatto l'operazione contro i software spia, denominata Exodus, con la Procura di Napoli, l'operazione di intercettazioni abusive con la piattaforma di Amazon che riceveva tutte le informazioni nel Cloud.

Key4biz. ***Come sono cambiati ed evoluti da una parte il modo di***

operare del Nucleo Speciale Privacy e Frodi Tecnologiche (GdF) e dall'altra come è cambiato il crimine informatico in questi tre anni?

Giovanni Reccia. L'attività del Nucleo è diventata molto più penetrante in questi tre anni rispetto a questi obiettivi assolutamente nuovi, soprattutto nel dark web e soprattutto rispetto all'illecito trattamento dei dati che sono stati considerati in una nuova ottica più di Polizia giudiziaria.

Invece, sotto il profilo del crimine informatico probabilmente c'è più consapevolezza dell'esistenza dei crimini informatici da parte dei cittadini. Tuttavia, non c'è ancora una cultura digitale adeguata, perché molto spesso sono i comportamenti errati che fanno sì che si cada in qualche trappola, in qualche truffa di cybercrime.

Key4biz. ***Quindi le persone non sono pronte a difendersi e a prevenire possibili attacchi informatici.***

Giovanni Reccia. C'è sicuramente ancora un problema di cultura digitale in Italia, che non è ancora molto diffusa sotto il profilo dei comportamenti in tema di sicurezza. Se c'è la necessità di aumentare gli investimenti delle imprese per la sicurezza informatica, allo stesso tempo non ci sono investimenti a largo raggio. Soltanto le aziende di dimensioni maggiori e più avanzate tecnologicamente investono in modo adeguato in sicurezza e cultura digitale. Il problema c'è in assoluto.

Key4biz. ***Come è cambiata in questi anni la cooperazione internazionale a livello investigativo?***

Giovanni Reccia. In questi tre anni l'attività di cooperazione a livello investigativo è esplosa. Abbiamo avuto rapporti sia con l'FBI americana, una delle più avanzate sotto il profilo del crimine informatico a livello mondiale, ma poi abbiamo instaurato attraverso le autorità giudiziarie italiane canali proficui con Eurojust. E poi c'è il lato, che è stato

ampliato, della collaborazione fra forze di polizia a livello europeo soprattutto con Europol. Quindi, un triplo canale. Fermo restando che si sconta sempre il problema del mancato scambio di informazioni tra polizie specialmente con paesi che non hanno aderito alla Convenzione di Budapest sul crimine informatico. Sono parecchi paesi, molti dei quali asiatici, dove spesso si riscontrano forti concentrazioni di botnet.

https://www.key4biz.it/giovanni-reccia-gdf-tre-anni-vissuti-intensamente-a-combattere-il-crimine-informatico/312891/

Cybersecurity, nuovo bando da 10 milioni di euro per proteggere l'Ue digitale

Pubblicato dalla Commissione europea il nuovo Invito a presentare progetti volti ad aumentare i livelli di cyber difesa delle infrastrutture strategiche e digitali dei Paesi membri dell'Unione, del valore complessivo di 10,5 milioni di euro.

Il bando, che è stato attivato tramite il Meccanismo per collegare l'Europa (CEF) 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.

"*L'invito pubblicato oggi contribuirà a rafforzare la nostra resilienza contro le minacce informatiche* – ha spiegato

Thierry Breton, Commissario per il Mercato interno – *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 a far progredire le tecnologie e le soluzioni innovative di cybersecurity in modo mirato*".

Per partecipare all'Invito c'è tempo fino al 3 novembre 2020.

Come spiegato sul sito del CEF, i migliori progetti saranno selezionati entro aprile 2021, mentre la ripartizione delle risorse finanziarie tra tutte le proposte sarà annunciata il mese successivo, a maggio 2021.

Secondo l'ultima edizione del "*Cybersecurity Exposure Index*", che costruisce la mappa globale della cyber resilienza e delle strategie di protezione informatica, **l'Europa si conferma cyber fortezza globale**, occupando gran parte dei posti in classifica nella Top20.

> *Cybersecurity, nuovo bando da 10 milioni di euro per proteggere l'Ue digitale*

Europa continente più cyber protetto del mondo, l'Italia

entra in Top 20

I Paesi meno esposti al mondo alle minacce del cyber crime sono la Finlandia, la Danimarca e il Lussemburgo. I più esposti, invece, sono Afghanistan, Myanmar ed Etiopia.

L'edizione 2020 del "***Cybersecurity Exposure Index***" costruisce **la mappa globale della cyber resilienza e delle strategie di protezione informatica** che ogni Paese ha nel tempo sviluppato e migliorato. Secondo l'indagine condotta da *Passwordmanagers.co*, l'Europa è il continente più cyber difeso del mondo.

La classifica

I primi 10 Paesi del pianeta meno esposti alle minacce informatiche sono Finlandia, Danimarca, Lussemburgo, Australia, Estonia, Norvegia, Giappone, Stati Uniti, Austria, Svizzera e Nuova Zelanda.

L'indagine si propone di valutare il livello di protezione informatica delle infrastrutture strategiche, tra cui quelle della trasformazione digitale, dei device e degli oggetti connessi in rete, delle identità digitali.

Ogni Paese (108 in totale) è stato valutato con un punteggio compreso tra 0 e 1, cioè da un'esposizione ai cyber attacchi pari sostanzialmente a zero ad un'esposizione invece piena.

"Nonostante le diverse capacità tecnologiche e la disponibilità immediata di risorse, la cyber sicurezza dovrebbe essere l'imperativo di ogni Nazione – ha spiegato nel commento ai dati **Josh Frisby**, fondatore di Passwordmanager.co – *perché già oggi sapere che nel Paese dove si risiede e si fa impresa i livelli di protezione informatica sono più elevati*

che altrove è un valore aggiunto”.

L’Italia nella cyber fortezza Europa

È evidente la superiorità numerica dei Paesi europei, che si conferma anche se prendiamo in considerazione la Top20, con il Belgio all’11° posto, seguito dalle Mauritius, dal Canada e dal Regno Unito a pari merito al 13° posto, dalla Spagna e dalla Svezia al 14°, dalla Francia, da Singapore, dalla Germania e dal Qatar al 17°, dalla Croazia e dall’Irlanda al 18°, dall’Olanda e dalla Slovacchia al 19° e dall’**Italia** e la Corea del Sud al 20°.

Il nostro Paese, nello specifico, occupa un’ottima posizione in questa classifica mondiale, meno in quella relativa all’Europa, dove siamo solo al 14° posto, con un indice complessivo di 0,269.

La **cyber fortezza Europa** è la meno esposta ai cyber attacchi, con un indice medio dello 0,329 e oltre il 70% dei propri Paesi poco o per niente esposti, seguita dal Nord America, con 0,462.

Sono invece maggiormente esposti ai cyber criminali il 34% circa degli Stati Uniti, il 40% dei Paesi sudamericani, il 60% di quelli asiatici e il 75% di quelli africani.

> *Europa continente più cyber protetto del mondo, l’Italia entra in Top 20*

Pagare le tasse con lo spyware, il connubio Stato-cyber crime

La tua banca ti invita a scaricare un'applicazione per pagare le tasse, ma all'interno è contenuto un malware che consente a chiunque l'accesso completo al network aziendale. È quanto denunciato da TrustWave, che ha soprannominato il malware in questione "***Goldenspy***".

La vittima è un'azienda cliente del provider servizi di sicurezza informatici. Il nome deriva dal termine ***spyware***, un tipo di software che raccoglie informazioni riguardanti l'attività online di un'organizzazione ma senza consenso, in maniera illecita.

Tasse e spyware

Il fatto, riportato ieri da *Cbsnews,* è accaduto in Cina e secondo **Brian Hussey**, vice presidente TrustWave ed ex specialista informatico dell'FBI: "*E' l'ennesimo caso di spionaggio industriale che dovrebbe farci capire quanto sia rischioso lavorare in Cina*".

Lo *spyware* si è attivato due ore dopo l'installazione del software per il pagamento delle tasse richiesto dallo Stato. Di fatto, in poco tempo i *cyber* criminali hanno utilizzato una *backdoor* per installare parallelamente il malware "*GoldenSpy*".

L'attacco è stato identificato da TrustWave ad aprile, ma non è stato specificato se è legato in qualche modo al Governo cinese o ad un gruppo criminale.

L’ente statale e i cyber criminali

Secondo Hussey, però, la complessità dell’attacco farebbe pensare ad un ente statale: “*Non sappiamo ancora se il nostro cliente sia l’unica vittima, o se ce ne sono altre, o se tutte le organizzazioni straniere su territorio cinese siano potenziali vittime*. *C’è da chiedersi se Pechino lo sapesse*”.

Un’accusa che ricorda molto da vicino quella del Premier australiano, Scott Morrison: “*Sappiamo che si tratta di un sofisticato attore statale a causa delle dimensioni e della natura degli obiettivi e della tecnica utilizzata*”.

A marzo 2020, la società di sicurezza informatica FireEye ha osservato un forte aumento di attività di *cyber* spionaggio economico, soprattutto a seguito del peggioramento delle relazioni USA-Cina.

A maggio, infine, gli Stati Uniti hanno accusato la Cina di aver hackerato un piano industriale di sviluppo di un vaccino contro il Coronavirus. Pechino ha immediatamente negato ogni coinvolgimento in queste pratiche di *cyber crime*.

Pagare le tasse con lo spyware, il connubio Stato-cyber crime

---

Cybersecurity, nasce il modello unico europeo di certificazione. Bilancio Ue:

1,34 miliardi per proteggere la transizione al digitale

Presentata ieri la proposta di bilancio dell'Unione europea. La Commissione ha valutato come ottimale un bilancio di 166,7 miliardi di euro per il 2021, a cui si aggiungono 211 miliardi in sovvenzioni e 133 miliardi in prestiti nel quadro del programma Next Generation Eu.

Questo bilancio, una volta adottato, sarà il primo del nuovo quadro finanziario pluriennale 2021-2027 e il primo bilancio annuale proposto dalla Commissione della Presidente **Ursula von der Leyen**.

Il Bilancio Ue e il digitale da proteggere

Di queste risorse finanziarie, **1,34 miliardi di euro dovrebbero essere spersi per il programma Europa digitale**, allo scopo di **potenziare le cyber difese** dell'Unione e favorire la transizione digitale.

Nello stesso bilancio, è stata avanzata la proposta di investire 10,13 miliardi di euro proprio in infrastrutture sostenibili, innovazione e digitalizzazione. Una parte dei fondi andrà al dispositivo per gli investimenti strategici per sviluppare l'autonomia strategica delle catene di approvvigionamento essenziali a livello europeo.

Il progetto di bilancio per il 2021, lo ricordiamo, si basa sulla proposta della Commissione per il prossimo bilancio a lungo termine dell'UE presentata il 27 maggio 2020.

Una volta che il Parlamento europeo e il Consiglio avranno trovato l'accordo sul quadro finanziario pluriennale 2021-2027, compreso il piano per la ripresa post Covid-19, la Commissione adeguerà di conseguenza la sua proposta di bilancio per il 2021 con una lettera rettificativa.

Nasce il Gruppo SCC per la cyber certificazione

Sempre in tema di cybersecurity, la Commissione e l'Enisa hanno annunciato la creazione dello *Stakeholders Cybersecurity Certification Group* (**SCCG**), un nuovo ente certificatore in materia di sicurezza informatica.

Il Gruppo aiuterà l'Unione a garantire elevati livelli di sicurezza nei prodotti e i sistemi digitali e informatici, ma diversamente dal passato attraverso un unico modello di certificazione, il che rende l'operazione più semplice e meno costosa.

Si riduce la frammentazione dei numerosi modelli fino ad ora in circolazione, si garantiscono livelli di cyber protezione più alti e affidabili, sia per il mercato, sia per le imprese.

Faranno parte dell'SCCG rappresentanti del mondo delle istituzioni europee, delle università, delle imprese, delle associazioni di categoria e dei consumatori.

La novità è da inserire nel progetto europeo per sviluppare le necessarie capacità di sicurezza informatica, per prevenire e contrastare le minacce e gli attacchi informatici in continua evoluzione, ma soprattutto per proteggere i nuovi asset strategici, tra cui le **reti 5G**.

https://www.key4biz.it/cybersecurity-nasce-il-modello-unico-europeo-di-certificazione-bilancio-ue-134-miliardi-per-proteggere-la-transizione-al-digitale/311718/