DarkHotel, chi sono gli Hacker del Wi-Fi e perché colpiscono gli Hotel

DarkHotel è un gruppo di Criminal hacker legati alla **Corea del Nord** che è attivo almeno dal 2007. Si tratta di un vero e proprio *omen-nomen* in quanto il gruppo ha ottenuto il suo nomignolo per aver compromesso il Wi-Fi e tutte le reti di vari hotel di lusso. A seconda delle occasioni possono anche chiamarsi **Tapaoux, Pioneer, Karba e Nemim**.

Un solo obiettivo

Il gruppo utilizza una combinazione di metodi altamente sofisticati per intrappolare le vittime, ma gli hack alberghieri continuano ad essere un obiettivo di alto valore.

La maggior parte degli hotel colpiti si trovano in Asia, ma non mancano le strutture che sono rimaste vittime di questi attacchi anche negli Stati Uniti e in Europa.

Le vittime dei Criminal hacker sono state identificate in Corea del Nord, Russia, Corea del Sud, Giappone, Bangladesh, Thailandia, Taiwan, Cina, Stati Uniti, India, Mozambico, Indonesia e Germania.

Mentre la prima campagna di spionaggio DarkHotel è stata scoperta dagli esperti di Cyber Security alla fine del 2014.

Il Modus operandi

Questo *Advanced Persistent Threat* si affida principalmente a campagne di **spear-phishing.** Il loro bersaglio? Sottrarre dati

sensibili dai top executive, tra cui CEO, Senior Vice-President, direttori vendite e marketing di varie organizzazioni, mentre soggiornano negli hotel di lusso.

Questi dirigenti di alto livello provengono principalmente dai settori manifatturiero, della difesa, dei capitali, farmaceutico, delle forze dell'ordine, dagli ranghi militari e di altri settori.

Per fare tutto questo gli aggressori sfruttano diversi metodi, compresi gli exploit zero-day per penetrare nei sistemi bersaglio.

Uno dei loro preferiti è una vulnerabilità Flash. Questo inizia il suo processo di hacking compromettendo le reti Wi-Fi.

Da qui, una volta che gli utenti si connettono alla rete, vengono rappresentati con una finestra di dialogo che chiede loro di installare un falso aggiornamento.

L'aggiornamento falso è in realtà un pezzo di malware con firma digitale.

Il Malware usato dal Gruppo nord coreano, come se non bastasse, arriva equipaggiato con svariati keylogger che sottraggono tutto il rubabile e lo trasmettono direttamente alla fonte dell'attacco.

È curioso notare come negli hotel, solitamente, queste installazioni di keylogger e malware sono distribuite in modo selettivo e a individui mirati.

Questo gruppo di Criminal Hacker sembra sapere in anticipo quando le vittime prescelte arriveranno nelle strutture dai loro hotel di lusso e in che data lasceranno l'hotel.

È questo il modus operandi degli aggressori: aspettare in attesa fino a quando le loro vittime arrivano e si connettono a Internet, come è stato efficacemente analizzato dagli

esperti di Cyber Security che hanno studiato le attività di DarkHotel.

Per fare questo il gruppo di Criminal Hacker viola tutti i sistemi degli hotel che mantengono tracciate e registrare le informazioni di check-in e check-out degli ospiti. Accedendo a questo all'elenco, gli aggressori sono in grado di raccogliere informazioni sui loro obiettivi principali. Gli aggressori possono accedere, tra l'altro, a informazioni quali l'orario di arrivo e di partenza previsto della vittima, il numero di camera e il nome completo.

Oltre ad inquinare le reti peer-to-peer per infettare le masse, DarkHotel utilizza una serie di certificati digitali per estendere il perimetro del loro attacco. Il gruppo sfrutta i certificati digitali scarsamente implementati per firmare il loro malcode.

Attualmente, stanno rubando e riutilizzando altri certificati legittimi per firmare il loro set di strumenti, per lo più backdoor e info stealer. La loro infrastruttura cresce e si restringe nel tempo, senza un modello coerente di configurazione. È allo stesso tempo protetta con una crittografia flessibile dei dati e mal difesa con funzionalità deboli e mal implementate.

Gli strumenti dei Criminal Hacker

Darkhotel ha solo l'imbarazzo della scelta quando si tratta di scegliere gli strumenti e le tattiche per compromettere una rete alberghiera. Tra questi:

- **Keylogger:** Visto e considerato come la maggior parte degli hotel hanno computer e reti accessibili al pubblico;
- **Malware:** li utilizzano installando un semplice downloader di malware o malware sul computer dell'ospite per raccogliere informazioni;

- **Zero day**
- **Spear-phishing:** DarkHotel utilizza questi attacchi targhettizzati ad hoc per diffondere malware

Come arginare la minaccia

Ovviamente per ogni problema sollevato dalle azioni di DarkHotel esiste una soluzione in grado di mettere dei paletti saldi e costruire il Cyber Security Framework adeguato. In primis, se la violazione è già avvenuta il primo passo da fare è seguire una procedura di Data Recovery.

Per testare la sicurezza dei propri network che, come abbiamo illustrato, sono una delle vie principali per DarkHotel di attaccare le proprie vittime è consigliata una regolare e periodica attività di *Network Scan.*

Si tratta di uno scan specifico e dettagliato che analizza l'IP di un network in modo da identificare le sue vulnerabilità e punti deboli. Questo strumento può essere usato da chiunque, che sia una multinazionale con centinaia e centinaia di computer – come una grossa catena di Hotel – o che sia una piccola azienda con un network di soli pochi dispositivi.

Assicurata la "tenuta" della rete, si deve passare a un'attenta attività di *Vulnerability Assessment*. Si tratta di un'analisi di sicurezza che ha l'obiettivo di identificare tutti le vulnerabilità potenziali dei sistemi e delle applicazioni. Come? Valutando il danno potenziale che l'eventuale "attaccante" può infliggere all'unità produttiva. Personale altamente qualificato, in un secondo momento, integra e verifica i risultati attraverso una meticolosa attività manuale. Queste attività hanno lo scopo di rifinire la ricerca evidenziando eventuali errori commessi durante il processo. Uno degli aspetti chiave di questa tipologia di analisi è l'isolamento tempestivo delle vulnerabilità reali. Uno strumento buono di Vulnerability Assessment permette

all’utente di avere un’overview aggiornata del livello di sicurezza degli asset IT. Ovviamente, questo è il punto di partenza per ottimizzare tutti gli sforzi di security management.

Da ultimo non c’è misura preventiva migliore del *Penetration Test.*

Questo, detto in parole povere, fa un “esame” dei punti deboli relativi ad una infrastruttura IT e, dopo averli scoperti, prova ad exploitarli in maniera sicura e controllata. Le vulnerabilità che sono oggetto d’esame da parte delle attività di Penetration Testing possono essere presenti nel software stesso in questi punti d’accesso:

- Flaws non intenzionali nel design del codice del software;
- Utilizzando il software in un modo per cui non è stato progettato;
- La non corretta implementazione della gestione della configurazione del software;
- Backdoor (porte sul retro) nel sistema operativo.

Le attività di *Penetration Testing* possono essere condotte sia attraverso processi automatici che manuali. Solitamente, il target di questa attività è focalizzato sui seguenti endpoint:

- Network endpoint;
- Dispositivi Mobile e Wireless;
- Network Security Device;
- Server;
- Altre aree esposte come il codice che sta dietro alle applicazioni.

Lo scopo di un Penetration Test, tuttavia, è quello di andare il più a fondo possibile nell’infrastruttura IT aziendale per arrivare agli asset elettronici di una azienda. L’obiettivo non è quello di colpire duramente il bersaglio al primo tentativo, ma è quelli di colpire anche più duramente nei

tentativi seguenti.

Prendendo questo come punto di partenza, possiamo stabilire che l'obiettivo principale di un penetration test sia quello di identificare chiaramente le vulnerabilità di sicurezza. Oltre a quanto appena detto, c'è una serie di altri obiettivi che il penetration test può raggiungere:

- Verificare la compliance delle policy di sicurezza;
- Testare la consapevolezza dello staff in materia di sicurezza;
- Controllare se e come un'organizzazione può affrontare un security breach.

Insomma, le soluzioni per arginare il fenomeno sono già presenti, ora a prendere le redini della situazione devono essere le università; il rischio dovrebbe già essere ben chiaro.

https://www.key4biz.it/darkhotel-chi-sono-gli-hacker-del-wi-fi-e-perche-colpiscono-gli-hotel/273905/

Sanità nel mirino del cybercrime, nel mondo attacchi in aumento del 31%

Il sistema sanitario di ogni Paese è sempre più il bersaglio preferito del c*ybercrime* globale. E' quanto hanno affermato i ricercatori Clusit a Verona, in occasione del mese della sicurezza informatica, che hanno presentato i dati dei primi

sei mesi del 2019. **Nell'85% dei casi gli attacchi informatici hanno sempre come obiettivo l'estorsione di denaro e questo segmento del crimine online è in crescita del 3,8%.**

Riguardo alla **sanità, gli attacchi sono in aumento del 31% e nei primi sei mesi dell'anno** in corso se ne sono contati 757, di cui 97 considerati gravi. Le tecniche di cybercrime utilizzate sono principalmente il *phishing* e il *social engineering*, con un'impennata del 104%, ma il *malware/ransomware* riamane sempre lo strumento di *cybercrime* più diffuso.

L'*healthcare cybersecurity market* è infatti in forte espansione a livello mondiale, con un numero crescente di azioni contro ospedali, cliniche, centri per la salute dei cittadini e centri di ricerca universitari. La spesa in soluzioni tecnologiche avanzate per la difesa delle infrastrutture, dei device, delle reti e dei database sanitari si è aggirata attorno ai 7,6 miliardi di dollari, durante lo scorso anno, secondo uno studio Reports and Data, ma **entro il 2026 gli investimenti in cyber sicurezza sanitaria sono stimati superare i 27 miliardi di dollari** a livello globale.

Più in generale, le violazioni dei dati diventano, di anno in anno, sempre più impattanti per le aziende dal punto di vista economico. Secondo il nuovo report di Kaspersky, dal titolo "*IT security economics in 2019: how businesses are losing money and saving costs amid cyberattacks*", **nel 2019 il valore dei data breach ha raggiunto la cifra di 1,41 milioni di dollari**, in aumento rispetto alla quota di 1,23 milioni di dollari registrata per l'anno precedente. Per far fronte a questa situazione, le grandi organizzazioni stanno investendo sempre più denaro nella sicurezza informatica: **quest'anno i budget aziendali per la sicurezza IT sono stati pari a circa 18,9 milioni di dollari**, un aumento sostanziale rispetto agli 8,9 milioni di dollari stanziati, in media, nel 2018.

Fondamentale, secondo gli esperti, attivare un ***Security***

operation center o Soc all'interno di ogni struttura. L'adozione di un Soc può dimezzare le eventuali perdite economiche derivanti dalle violazioni dei dati, portandole ad avere un impatto medio di circa 675.000 dollari.

Altrettando utile è l'assunzione di un Dpo (***Data protection officer***), un dipendente responsabile della creazione e dell'implementazione di una strategia di protezione dei dati all'interno dell'azienda stessa, nonché della gestione di eventuali problemi di conformità. L'indagine ha evidenziato che più di un terzo delle organizzazioni (34%) che ha subito una violazione dei dati e che ha un Dpo all'interno non ha subito alcuna perdita di tipo economico.

> *Sanità nel mirino del cybercrime, nel mondo attacchi in aumento del 31%*

Cybersecurity, Profumo (Leonardo): 'Serve cooperazione in Europa'

Horizon 2020, **Pesco** (Permanent structured cooperation), **Edf** (European development fund) e policy come **Nis** (Network and information systems) e **Gdpr** (General data protection regulation) sono alcuni degli strumenti europei che hanno promosso e rafforzato la collaborazione tra le diverse organizzazioni, con importanti risultati. Sono questi, secondo l'amministratore delegato di **Leonardo Alessandro Profumo**, i principali strumenti giuridici su cui puntare per rafforzare la cybersecurity nel Vecchio Continente e sviluppare una vera

“indipendenza digitale”.

Inoltre, scrive Alessandro Profumo nel suo intervento a firma pubblicato oggi sul Sole 24 Ore, *“l’Italia, sfruttando anche un efficace modello di collaborazione pubblico-privato per la definizione di aree di potenziale vulnerabilità e eccellenze tecnologiche esistenti, è arrivata, forse prima di altri, alla definizione di un “perimetro cibernetico nazionale”, cioè all’individuazione di quanto di più cruciale per la vita di una Nazione, garantendo protezione cittadini, imprese e istituzioni.*

Molto quindi è stato fatto, ma il percorso da fare è ancora lungo. Vincere la sfida della cyber security non solo ci permetterà di proteggere quello che abbiamo oggi, ma è condizione fondamentale per creare solide basi di una reale indipendenza digitale. Solo operando oggi scelte corrette e coraggiose saremo in grado di sviluppare e valorizzare quelle competenze che renderanno possibile una crescita economica e sociale, attraverso la diffusione in sicurezza di tecnologie e servizi del futuro.”

Studi di settore, secondo stime di Leonardo. evidenziano che **a livello globale i cyber attacchi gravi sono aumentati nell’ultimo biennio di dieci volte rispetto a quello precedente, con 1.552 attacchi nel solo 2018**. Sono inoltre cresciuti del 57% i crimini di spionaggio cyber con finalità geopolitiche o di tipo industriale, tra cui il furto di proprietà intellettuale. Il mercato della sicurezza informatica sta attraversando una fase di boom, con un valore globale stimato di circa 180 miliardi di dollari nel 2021.

Cybersecurity, Profumo (Leonardo): ‘Serve cooperazione in Europa’

Telecamere di sicurezza, ecco perché possono essere a rischio hacker

Da tempo diversi ricercatori ed esperti si lamentano della scarsa sicurezza delle telecamere di sicurezza. Montate per lo più in bella vista per fungere da deterrente per possibili intrusioni, molte di esse vengono invece sfruttate come armi di offesa da parte degli hacker. Secondo *Fortune.com*, l'ultima moda in fatto di attacchi hacker, basata sulla vulnerabilità che consente ai malintenzionati di depistare il traffico di centinaia di migliaia di telecamere tramite attacchi Ddos, che molto semplicemente metto ko le telecamere che finiscono offline finché non viene pagato un riscatto.

Un allarme sicurezza sul rischio di attacchi massivi a telecamere di sicurezza è stato lanciato mercoledì scorso da Akamai.

Un nuovo obiettivo dei criminali sono anche le telecamere a circuito chiuso, utilizzate soprattutto in ambito televisivo. I modelli vulnerabili secondo gli esperti di Akamai sono prodotti dalle cinesi Hikvision e Dahua e dalla brasiliana Intelbras.

Quando questi dispositivi disegnati per restare su una Lan finiscono online sulla rete Internet pubblica, gli hacker sono in grado di ridirigere il traffico e bloccarne il funzionamento anche perché l'azionamento a distanza non è previsto.

Che fare per proteggere i device? Forse, prosegue Fortune, la cosa migliore sarebbe che i produttori munissero i dispositivi di strumenti di aggiornamento automatico, per la realizzazione di patch. Una eventualità non certo dietro l'angolo e che comunque non risolvere il problema alla radice, vista la quantità di telecamere installate che ci sono in giro.

> *Telecamere di sicurezza, ecco perché possono essere a rischio hacker*

Sicurezza cibernetica, perimetro allargato a 5G e società quotate

Il Governo italiano, come auspicato da tempo, crea finalmente un vero perimetro di sicurezza cibernetica, dotandosi di strumenti normativi che consentono al nostro paese di intervenire in maniera più tempestiva in caso di minacce e pericoli per la sicurezza nazionale provenienti dal cyberspazio. E' questo in sintesi il senso del decreto legge varato dal Consiglio dei ministri recante appunto **'disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica'** che allarga il suo ambito di applicazione al 5G e alle società quotate in Borsa.

Il decreto, sottolinea la nota della presidenza del Consiglio diffusa al termine della riunione dell'esecutivo, *"mira ad assicurare un livello elevato di sicurezza delle reti, dei*

sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione".

Perimetro di sicurezza cibernetico allargato

"Il varo del decreto che allarga il perimetro di sicurezza cibernetica è una mossa auspicata da tempo – dice **Stefano Mele**, avvocato e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano – *per creare nel nostro paese un piano normativo e politico più ampio per la sicurezza cibernetica*".

Il provvedimento appena varato si inserisce e integra la direttiva europea NIS (Network and Information Security) che si rivolge a società che forniscono servizi essenziali e grandi società del mondo digitale (motori di ricerca, aziende Cloud ecc.). *"Il nuovo perimetro di sicurezza cibernetica copre una serie di vuoti lasciati dalla direttiva NIS, in particolare le società di servizi essenziali pubbliche e private non coperte dalla direttiva europea, che ora saranno invece inserite nel nuovo perimetro di sicurezza cibernetica perché strategiche per la sicurezza nazionale".*

A breve sarà varato un decreto ad hoc che definirà i nomi delle aziende sensibili per la sicurezza nazionale che saranno inserite nel nuovo perimetro e che si aggiungono alle 465 società già individuate e coperte dalla direttiva NIS.

Golden power sul 5G

L’inserimento della norma sul golden power sul 5G nel decreto sul perimetro della cybersecurity dimostra l’urgenza della materia, dopo che il decreto ad hoc era scaduto il 9 settembre. Una materia troppo importante per restare in sospeso, in cima all’agenda del Conte bis, come dimostra la sua applicazione nei confronti delle telco (fra cui le cinesi Huawei e ZTE) in occasione del primo Consiglio dei Ministri della sua era. *“Il via libera al golden power sul 5G è volto a bloccare eventuali infiltrazioni in Italia di soggetti esteri potenzialmente pericolosi per la sicurezza nazionale* – aggiunge Stefano Mele – *il nuovo perimetro di sicurezza nazionale allarga l’applicazione dei poteri speciali del golden power in mano al presidente del Consiglio ai fornitori di hardware, software e attrezzature per il 5G. Si tratta quindi di un nuovo strumento normativo molto forte in mano al Governo per combattere il rischio di infiltrazioni nel nostro cyberspazio”.*

Infine, il decreto prevede che il presidente del Consiglio abbia il potere in caso di crisi cibernetica, su indicazione del **Comitato interministeriale per la sicurezza della Repubblica (CISR)** di intervenire rimuovendo la fonte della minaccia e quindi di reagire ad una minaccia difendendosi ma anche attaccando.

La nuova normativa prevede l’obbligo di comunicare sempre un attacco informatico, l’obbligo di controllare il procurement di forniture che rientrino nel perimetro di sicurezza cibernetica. Sono previste inoltre sanzioni che possono variare da 200mila euro a 1,8 milioni di euro.

Per saperne di più: 5G

> *Sicurezza cibernetica, perimetro allargato a 5G e società quotate*

Huawei sospesa dal team globale specializzato in cybersecurity. Meno preparata per le patch di sicurezza?

Huawei è stata sospesa dal **First** (Forum of Incident Response and Security Teams*)*, organizzazione nata negli anni ’90 per incoraggiare la cooperazione internazionale nel prevenire e contrastare gli episodi di hacking. Questo forum, fa parte del gruppo di **CERT** (*Computer Emergency Response Team*), è cresciuto così tanto da diventare una sorta di prima risposta informale a grandi attacchi globali e incidenti di sicurezza informatica. Ne fanno parte governi, esperti del settore e società multinazionali. Il consiglio di amministrazione del gruppo comprende rappresentanti di **Cisco**, **Hitachi**, **Siemens** e **Juniper** Networks. Il braccio destro della cybersecurity del Dipartimento di sicurezza Usa e il Centro nazionale di sicurezza informatica del Regno Unito sono entrambi membri.

Un portavoce di Huawei, riporta il *Wall Street Journal*, ha dichiarato che la società non commenterà la sospensione e ha aggiunto che gli Stati Uniti *“utilizzano tutti gli strumenti a loro disposizione”* per interrompere le operazioni e il business della tlc cinese. Infatti la decisione presa dal First deriva dal bando Usa nei confronti di Huawei.

I rischi per Huawei dopo la sospensione dal Forum globale specializzato in cybersecurity?

La sospensione dal forum globale, specializzato nel contrasto dei cybercrime, potrebbe costare alla società cinese *"un rallentamento nella realizzazione delle patch di sicurezza"*, scrive il Wall Street Journal, perché *"i membri del First condividono informazioni e intelligence per identificare e isolare rapidamente attacchi informatici o vulnerabilità e diffondere informazioni per proteggerli dalla loro rapida diffusione".* Non facendone più parte Huawei è costretta ora ad affrontare da sola gli attacchi e possibili violazioni della sicurezza informatica. Inoltre la società cinese non avrà più accesso a discussioni riservate all'interno dei cosiddetti gruppi di interesse speciale del First. Tali gruppi condividono i dettagli sulle vulnerabilità della cibersicurezza tra le organizzazioni membri. Infine, a Huawei sarà vietato di utilizzare una piattaforma automatizzata per condividere informazioni sul malware.

> *Huawei sospesa dal team globale specializzato in cybersecurity. Meno preparata per le patch di sicurezza?*

Come gestire un attacco informatico e quali errori

non fare. Il truck di IBM

Simulare un cyber attack, è un modo per capire come le aziende potrebbero reagire ad un eventuale attacco informatico imparando a gestire lo stress e a difendersi da un possibile data breach.

Tutto questo è opera di **IBM** che ha investito 200 milioni di dollari nella costruzione del'**X-Force Command Cyber Tactical Operations Center** (C-TOC), una sala operativa cyber su ruote, approdata al **Politecnico di Milano,** in piazza Leonardo da Vinci (dove rimarrà fino al 20 settembre).

X-Force Command C-TOC

[embedded content]
L' X-Force C-TOC è un **Cybersecurity Operation Center** basato sul modello dei centri operativi tattici utilizzati dalle postazioni di comando militari. La struttura mobile contiene un centro di sorveglianza, un data center e strutture per conferenze in grado di ospitare oltre venti operatori tra analisti e personale.

L'autoarticolato, equipaggiato con alimentazione autosufficiente e comunicazioni satellitari e cellulari, offre una rete sterile e resiliente per indagini sugli incidenti informatici e relativa risposta.

"*Grazie all'X-Force andiamo a creare una simulazione immersiva e integrale per far testare alle aziende la risposta ad un attacco informatico*", ha spiegato **Francesco Teodonno**, IBM Security Leader per l'Italia. *"Gli attacchi al giorno d'oggi sono diventati molto più sofisticati, non parliamo di malware ma di veri e propri sistemi di attacco. Quindi per affrontare*

una sfida di questo tipo bisogna essere preparati a saper prendere l'attacco".

La simulazione

Durante la simulazione cerchiamo di prendere in considerazione più punti di vista. Non solo l'aspetto tecnico, ma anche la gestione degli aspetti di leadership, di gestione del rischio, di gestione della comunicazione, di policy e la relazione che c'è con i media", ha spiegato durante la simulazione **Pompeo D'Urso**, C-TOC Technical Leader di IBM Security. *"E' quello che facciamo nella nostra tipologia di sessione, orientata quindi alla leadership e alla Business Relationship Responsive, nella quale l'azienda deve vedere il livello di preparazione nel caso in cui devono interagire anche con enti esterni.*

La sala operativa dell'X-Force durante la simulazione

"E' in virtù di tutta una serie di possibili attacchi – continua Pompeo – *come ad esempio problemi con i bancomat, problemi con la divulgazione online dei dati degli utenti e di quanti questi abbiamo un impatto sulla brand reputation, che ne può derivare un danno economico. Quindi bisogna considerare più punti di vista e allenarsi il più possibile per essere pronti ad affrontare nel momento in cui si è esposti ad un cyber attack".*

> *#CToc #CyberSecurity #IBM a #Milano in collaborazione con @polimi: #presstour e simulazione di un #CyberAttack: come gestire al meglio un attacco informatico. pic.twitter.com/vV4OlCAx9D*
>
> *— IBM Italia (@IBMItalia) September 12, 2019*

Formazione e mancanza di cyberskills

La funzione del camion C-TOC non è solo quella di aiutare le aziende nella loro formazione sulla sicurezza informatica, ma anche di fornire uno scopo educativo per aiutare a colmare il crescente divario delle **cyberskills**.

Portando il camion C-TOC nelle scuole e nelle università, IBM si augura di incoraggiare sempre più studenti a prendere in considerazione una carriera nel settore della sicurezza informatica.

L'X-Force Command C-TOC di IBM in piazza Leonardo Da Vinci a Milano
Nei prossimi giorni saranno ospiti del truck anche gli studenti del Politecnico che potranno provare le simulazioni **il 19 settembre**. Partito dagli Usa nel 2018 e dopo aver toccato le principali città europee, il truck andrà alla volta di Madrid per l'ultima tappa del suo tour europeo.

https://www.key4biz.it/come-gestire-un-attacco-informatico-e-quali-errori-non-fare-il-truck-di-ibm/270613/

Smart city vulnerabili: si spenderanno solo 135 miliardi

in cyber sicurezza entro il 2024

Nel 2018 gli attacchi informatici a livello globale, "*con impatto significativo*" o di livello critico elevato, sono aumentati del 40% quasi. I settori che più di altri hanno registrato un incremento sensibile delle attività cyber criminali sono stati quelli della ricerca e della formazione, che hanno visto una crescita degli attacchi del 55% rispetto al 2017; ma anche dei servizi online/cloud e delle banche, con l'aumento degli attacchi rispettivamente del 36% e del 33%.

I dati contenuti nel Rapporto Clusit 2019 hanno posto in evidenza che **le infrastrutture critiche risultano essere i settori per i quali i rischi cyber sono cresciuti maggiormente** durante l'anno passato.

Un dato che deve preoccupare, non tanto per le tecniche utilizzate dai cyber attori in campo, né per la loro forza distruttiva, quanto per il raggio d'azione che possono raggiungere (a quanto pare illimitato) e per la loro efficacia.

Altro motivo di preoccupazione è che le **tecnologie della trasformazione digitale** o della cosiddetta "*Terza piattaforma*", tra cui Internet delle cose, intelligenza artificiale, realtà aumentata/virtuale, stampa 3D, blockchain, cloud e big data, presentano troppe **vulnerabilità**.

L'allarme è stato lanciato da uno studio ABI Research, secondo cui questi sistemi risultano ancora oggi troppo facilmente attaccabili, anche a causa delle attuali difficoltà di monitoraggio e gestione dei sistemi, andando ad individuare un'evidente fragilità della società digitale.

A sistemare le cose potranno essere solo le nostre scelte in ambito di cybersecurity.

Le città sono già oggi il motore economico, economico e politico primario di ogni Paese. in alcune nazioni sono sorte delle vere e proprie Città Stato, con decine di milioni di abitanti. D'altronde, la popolazione urbana è in rapida crescita in tutto il mondo e le megalopoli con oltre 10 milioni di abitanti saranno decine entro il 2050, con vere e proprie aree urbanizzate estese con oltre 30 milioni di cittadini.

Entità demografiche straordinarie, che richiedono capacità organizzativa e d'azione altrettanto straordinarie.

È proprio in queste città in espansione che si innestano alla perfezione le tecnologie della Terza piattaforma ed il loro uso si farà massiccio entro pochissimo tempo, dando vita ad una rete di ***smart cities*** globali. Secondo molti esperti, l'arrivo del 5G nel 2020 cambierà completamente lo scenario, dando il via definitivamente alla concreta trasformazione digitale della nostra società.

La criticità principale, però, sta nel fatto che **alla spesa per l'innovazione digitale non sta non corrispondendo un equivalente investimento in tecnologie per la sicurezza informatica e la cybersecurity** nel suo complesso.

Lo studio ABI Research ha stimato in **135 miliardi di dollari la spesa in cyber sicurezza a livello mondiale entro il 2024**. Una **cifra considerata insufficiente**, che lascia ancora aperte troppe vulnerabilità, ben evidenti proprio nelle smart cities.

Alle infrastrutture critiche come energia, risorse idriche, pubblica sicurezza, rifiuti, trasporti e sanità andrà solo il 44% della spesa riportata dal Rapporto, davvero poco.

Le *smart cities* accoglieranno al loto interno più di 1,3 miliardi di connessioni Lpwan (*Low-power wide-area network*)

entro il 2024, tecnologie di rete che richiedono bassi consumi e ridotta velocità di trasferimento dati, in grado di garantire ampia copertura, potenzialmente persino superiore rispetto a quella di una cella di telefonia mobile, utilizzando una potenza inferiore, ma anche non abbastanza evolute e potenti da gestire "*anche*" il crescente numero di attacchi informatici che le riguardano.

C'è da aggiungere che i progetti smart city stanno crescendo ovunque e certamente mirano ad aumentare la rete di infrastrutture locali. Secondo un nuovo studio di Verified Market Research, dal titolo "*Global Smart City ICT Infrastructure Market Size and Forecast To 2026*", **entro il 2025 il mercato delle infrastrutture ICT per le città del futuro raggiungerà il valore di 1.714 miliardi di dollari**, con un tasso di crescita annuo (Carg 2018-2025) del 17,5%.

Una cifra enormemente più alta rispetto a quanto si stima sarà speso per la cybersecurity a livello mondiale.

> *Smart city vulnerabili: si spenderanno solo 135 miliardi in cyber sicurezza entro il 2024*

It-sa 2019: le nuove sfide della cybersecurity? Il punto a Norimberga dall'8 al 10 ottobre

Nuovi modelli di pagamento, interconnessione globale delle catene di produzione, eHealth. La digitalizzazione migliora il

nostro modo di vivere e lavorare ma nasconde anche molte insidie: i crimini informatici minacciano ogni settore e sono in costante evoluzione e aumento.

Da qui l'importanza di un evento quale è **it-sa**, che con circa 700 espositori nel 2018 è **la più grande manifestazione fieristica B2B dedicata alla cybersecurity** contribuendo annualmente alla diffusione delle ultime soluzioni e innovazioni. L'ultima edizione ha ospitato oltre 14 mila visitatori e per diversi anni it-sa ha registrato una crescita a due cifre di espositori e visitatori a riprova del grandissimo interesse per il settore. Per rispondere alla crescente richiesta, it-sa 2019 vedrà l'aggiunta del padiglione 11.

Ancora una volta, come negli anni precedenti, saranno presenti le aree **Startup@it-sa,** pavillion di vari paesi e un ampio programma di circa **350 presentazioni** che faranno chiarezza su questioni quali aspetti giuridici, tendenze, uso di intelligenza artificiale, IT security per l'industria 4.0 e le infrastrutture critiche.

Il 7 ottobre, giorno precedente l'apertura di it-sa, inizieranno inoltre a Norimberga come da tradizione il congresso **Congress@it-sa** con la conferenza annuale degli IT Security Officer a livello statale e municipale e **UP19@it-sa**, competizione tra start up per convincere una giuria di esperti e investitori e vincere un coaching individuale con Digital Hub Cybersecurity e l'IT Security Cluster Bavarese.

L'**elenco degli espositori 2019** e il **programma collaterale** completo sono disponibili sul sito www.it-sa.de/en rispettivamente alle sezioni *Exhibitors & Product* e *Programme*.

Biglietti gratuiti

Iscrivendosi alla newsletter di it-sa è possibile ricevere un biglietto gratuito giornaliero per la manifestazione. Ulteriori biglietti sono acquistabili online.

Tutti gli eventi sulla sicurezza firmati NürnbergMesse

NürnbergMesse conferma il proprio know-how in ambito sicurezza portando avanti svariati eventi B2B che coprono ogni aspetto del comparto: accanto a *it-sa* e *it-sa India*, fanno parte del security cluster anche *Enforce Tac* (Law Enforcement), FeuerTrutz e FIRE & SECURITY INDIA EXPO (Prevenzione Antincendio), Perimeter Protection (Protezione perimetrale di aree aperte ed edifici) e U.T.SEC (Droni e Tecnologie a controllo remoto per la sicurezza) per un totale di circa 1,600 espositori e 41,000 visitatori da tutto il mondo.

Riferimenti in Italia

Chiunque desiderasse maggiori informazioni sull'evento può contattare la Filiale Italiana dell'Ente Fieristico NürnbergMesse Italia Srl al numero 02 36753260 o per email info@nm-italia.it

> *It-sa 2019: le nuove sfide della cybersecurity? Il punto a Norimberga dall'8 al 10 ottobre*

Non ci sono più gli hacker di una volta

Nel variegato mondo delle minacce di sicurezza informatica uno dei pericoli più insidiosi è sicuramente il **Remote Access Trojan (RAT)**.

Si tratta di un programma malware che lavora includendo una back door per il controllo amministrativo del computer bersaglio.

Una delle inside principali è proprio l'abilità del **RAT** di essere scaricato in modo invisibile con un programma richiesto dall'utente – che si tratti di un'applicazione, un gioco o un semplice PDF – o inviato come allegato a un'e-mail.

Una volta che il sistema host è compromesso, l'intruso può usarlo per distribuire RAT ad altri computer vulnerabili e creare una botnet.

Adwind: il più pericoloso

Esistono, come per tutti i malware, vari tipi di RAT, ma non c'è dubbio che il più "completo" sia **Adwind**, grazie alla sua capacità di sottrarre informazioni dai sistemi bersaglio, di crittografare file e di impossessarsi delle credenziali **VPN**.

Come se non bastasse, nelle sue ultime release, è stata aggiunta l'abilità di fare keylogging, screenshot, registrare video dalla webcam del pc bersaglio e audio dal microfono.

Scoperto per la prima volta nel 2012 – al tempo era noto come Frutas – Adwind mantenendo la sua struttura è anche chiamato

AlienSpy, Unrecom, Sockrat, JSocket e **JRAT**. Nel suo primo picco di attività (2013-2016) è stato indicato come il colpevole di quasi 160 campagne di attacco nei confronti di oltre 70mila target.

Tra queste spicca quella portata avanti da AlienSpy sul finire del 2015 che ha preso di mira tutti i maggiori player nel settore della finanza e delle TelCo statunitensi oltre ad alcuni enti governativi attraverso delle campagne di phishing mirate. All'interno delle e-mail incriminate il malware era ben nascosto nei panni di fatture, note spesa o addirittura ordine da parte di fornitori.

La facilità con cui era riuscito a diffondersi era anche in parte dovuta all'abilità del malware di funzionare su tutte le principali piattaforme disponibili sul mercato: da Windows a Mac, passando per Linux e Android.

Bersagli diversificati

Se inizialmente Adwind sembrava avere come bersaglio unicamente i settori citati poco prima, di recente, secondo uno studio pubblicato da un'università americana, il malware è cominciato ad apparire come il principale indiziato in attacchi che hanno coinvolto oltre 1.500 organizzazioni di oltre 100 Paesi; organizzazioni che andavano dal settore dell'industria pesante fino ai piccoli studi legali. Un pattern che non sembra seguire particolari "agende" come spesso accade quando alle spalle di queste campagne ci sono gruppi hacker sponsorizzati. Nel 2017 è comparso dopo una serie di incidenti che hanno coinvolto le principali aziende del settore aerospaziale europeo, preambolato da una attenta strategia di social engineering. Nel 2018 ha sfruttato una vulnerabilità di Autodesk A360 per ottenere il controllo numerosi sistemi. Nel 2019 è stato trovato in oltre 2 milioni di email di phishing.

Il Cyber crimine diventa SaaS

Uno dei motivi per questa apparente randomizzazione degli attacchi è dovuta al fatto che Adwind, nelle sue versioni **JSocket**, è da qualche tempo distribuito nel dark web, in una sorta di perverso e-commerce del Cyber crimine.

I prezzi variano dai 30 dollari per il pacchetto contenente il Malware pronto ad essere lanciato (solo per un mese) fino ai 200 per una licenza illimitata, una sorta di crimine as a service; il tutto – ovviamente – corredato di supporto tecnico e assistenza via mail.

Sfortunatamente il fenomeno non è limitato ai soli RAT: il mercato del Dark web è diventato un vero e proprio retail che opera su piattaforme, non troppo differenti da un qualsiasi e-shop, che permettono di recensire i "prodotti", lasciare una valutazione e ottenere garanzie di acquisto, il tutto incorniciato con un'interfaccia intuitiva e responsive facilmente navigabile. Non mancano neppure elementi di customer care, come accennato, che comprendono FAQ, chat di supporto e dettagliate pagine di aiuto.

Oltre ai già i citati RAT si possono trovare Decrittatori di Password, campagne di Phishing pre-confezionate, keyloggers e pacchetti completi "end to end" che comprendono tutti gli elementi necessari a compiere frodi bancarie. Naturalmente in questo mondo regnano le cripto valute, per loro natura difficili da tracciare.

Gli esempi qui elencati sono solo la punta dell'iceberg di un mondo che, nonostante i migliori tentativi delle autorità preposte, sembra essere solo in crescita.

Oggi, esistono decine di piattaforme che vendono software come i malware e per ogni sito che viene abbattuto un altro eventualmente prende il suo posto.

È stato stimato che nel 2017 negli Stati Uniti d'America le frodi commesse online hanno causato circa 17 miliardi di dollari di perdite ad aziende e privati, mentre in Europa l'Italia si piazza in seconda posizione per numero di crimini subiti.

È sicuramente utopistico augurarsi di poter debellare completamente le attività criminose, ma alcune accortezze da parte del consumatore possono aiutare a scongiurare questi attacchi.

Una delle misure più semplici parte dall'igiene delle password: una password sicura non deve essere scontata, non deve richiamare al tuo nome/data di nascita o a quello dei tuoi cari, non deve essere eccessivamente corta e deve includere caratteri speciali.

Un altro consiglio è quello di utilizzare, laddove possibile, un sistema autenticazione a due fattori, che assicura un'ulteriore barriera di protezione anche nel caso in cui venga sottratta la password.

Sono regole semplici da seguire, ma che possono migliorare drasticamente la resilience dei propri sistemi e dispositivi.

Sparisce la barriera d'ingresso

Ma facendo un passo indietro, la preoccupazione più grande è inerente alla facilità di accesso per attori malintenzionati agli strumenti necessari per compiere crimini on-line.

La scena del Criminal hacking fino a pochi anni fa era stata dominata da un substrato di persone in possesso di un certo livello di *skill*.

La recente ondata di pacchetti e soluzioni *ready made* rischia di inondare il web di aspiranti Criminal hacker che ora non hanno necessariamente le competenze e le conoscenze necessarie per portare avanti campagne di phishing o di malware da soli,

ma che grazie ai servizi del Dark Web si trovano le soluzioni già preconfezionate e pronte ad essere utilizzate.

La democratizzazione del Cyber crime, quindi, sembra essere alle porte.

https://www.key4biz.it/non-ci-sono-piu-gli-hacker-di-una-volta/269783/