Infrastrutture critiche, come proteggere quelle nazionali? Intervista a Danilo Gismondi (Trenitalia) e Riccardo Barrile (Gruppo FS)

La cybersecurity ha ormai un ruolo centrale all'interno di ogni contesto aziendale. In particolar modo per la protezione delle infrastrutture critiche, dove investimenti sempre più importanti, per far fronte al crescente numero di violazioni, portano le aziende a concentrare la sicurezza nelle mani di specialisti esperti. E allora quanto è importante la cultura della sicurezza per la protezione dell'intero Sistema-Paese? Ne abbiamo parlato con **Danilo Gismondi** – Chief Information Officer – Trenitalia SpA, e **Riccardo Barrile** – Chief Security Officer – Gruppo FS.

Key4biz. ***Quanto è importante la sicurezza e la protezione delle infrastrutture critiche oggi?***

Danilo Gismondi e Riccardo Barrile. È un elemento imprescindibile anzi, è parte integrante della missione delle aziende che erogano servizi critici per il Paese. La cultura della sicurezza, che si tratti di esercizio operativo (es. servizi di trasporto), protezione dell'infrastruttura fisica o di sistemi tecnologici preposti alla erogazione di un servizio, rappresenta un pilastro trasversale senza il quale nessun piano industriale potrebbe realizzarsi nel corso del tempo. La sicurezza logica, dopo l'iniziale fatica ad imporsi negli anni '90 ed inizio 2000, è vista non più come una voce

di spesa “necessaria”, ma come una leva di business vera e propria. Che si tratti di sistemi commerciali o di tecnologie industriali, è ormai un fatto ineluttabile che i processi aziendali debbano svilupparsi grazie alla leva digitale e che quest’ultima debba fondarsi su un approccio alla sicurezza *by design*. La tecnologia è l’elemento di snodo: il ricorso sempre più imponente all’**IoT,** a paradigmi di condivisione tra imprese e tra imprese e cittadini, all’uso di Intelligenza artificiale nei processi industriali o di *customer engagement*, rappresentano grandi opportunità, ma celano rischi nuovi e minacce complesse da fronteggiare. Su questi aspetti riteniamo indispensabile mantenere alta l’attenzione attraverso il coinvolgimento continuo e fattivo delle strutture di cybersecurity.

Key4biz. ***Come funziona il modello di Governance & service per la sicurezza informatica all’interno di Ferrovie dello Stato?***

Danilo Gismondi e Riccardo Barrile. Il **Gruppo Ferrovie dello Stato Italiane**, come infrastruttura critica nazionale, non può permettersi nessun rischio che possa portare a disservizi e interruzioni nell’erogazione dei propri servizi e per far fronte a tale necessità, adotta un approccio di tipo proattivo e preventivo, basato sul *framework* internazionale **NIST** *(National Institute of Standards and Technology of US)*.

Già nel 2017 la funzione di cybersecurity del Gruppo FSI ha avviato un processo di riorganizzazione in linea con il nuovo quadro normativo nazionale e internazionale in materia di cybersecurity. Tale processo prevede un piano di internalizzazione di risorse e servizi di sicurezza informatica precedentemente forniti ed erogati da *outsourcer*.

Tra le innovazioni principali vi è la realizzazione del nuovo

Security Operation Center (**SOC**) che eroga centralmente i servizi di cybersecurity per le Società del Gruppo FSI. Nonché l'utilizzo di strumenti cognitivi dotati di intelligenza artificiale per l'analisi delle minacce rivolte al Gruppo FS.

Il modello di Governance attuato in FSI è di tipo circolare con la struttura di cybersecurity di Gruppo che, oltre a definire linee guida e politiche in materia di sicurezza informatica, offre anche servizi operativi attraverso il suo SOC. Trenitalia, così come le altre società del Gruppo, opera in sinergia con la struttura Cyber, avvalendosi dei servizi di sicurezza logica e integrandoli nei processi ICT aziendali, in tutte le fasi del ciclo di vita del software e delle IT Operations. Tutto ciò genera una interazione continua, agevolata anche attraverso processi di *co-location*, che porta ad accorciare la catena decisionale e ad accelerare i processi di trasferimento di *know-how*

Key4biz. ***Purtroppo sono ancora poche le aziende che hanno nel proprio organico una figura con una responsabilità specifica come la vostra. Quali sono oggi le principali sfide per i Security e Information Officer?***

Danilo Gismondi e Riccardo Barrile. In realtà le grandi aziende già da tempo hanno maturato la giusta consapevolezza sull'importanza di avere nel proprio organico il *Security Information Officer* anche in virtù del nuovo quadro normativo ma anche del crescente livello della minaccia cyber che non lascia molto spazio all'improvvisazione.

Il problema dell'assenza di tale figura si avverte nelle **PMI** che svolgono spesso attività per le infrastrutture critiche e spesso non hanno un'adeguata protezione dei propri sistemi informativi. Questa criticità rischia di vanificare tutti gli sforzi fatti dalle grandi imprese per mantenere un adeguato

livello di protezione informatica.

Il rapido evolversi delle minacce informatiche impone al **CISO** una conoscenza approfondita non solo delle tematiche di *cybersecurity* ma anche del business da proteggere. Ritengo che la corretta interpretazione moderna del ruolo del CISO sia appunto quella di considerarsi parte dei processi dell'azienda, modificandosi dinamicamente in funzione delle strategie di business, evitando di porre rallentamenti o blocchi ma, piuttosto introducendo elementi di *security by design* già in fase di progettazione dei nuovi sistemi e/o applicazioni.

A tal fine è importante che il CISO organizzi momenti di scambio informativo con le altre funzioni dell'azienda al fine di aumentare il livello della consapevolezza sui temi della cyber sicurezza.

Key4biz*. **Il 16 maggio scorso è stato approvato in Consiglio dei Ministri il Decreto Legislativo per attuare in Italia la Direttiva NIS entrata in vigore il 26 giugno. Ora l'attuale quadro normativo e gli ambiti di applicazione previsti dal Decreto garantiscano un adeguato livello di protezione?***

Danilo Gismondi e Riccardo Barrile. Certamente l'introduzione della direttiva si aggiunge ad altri strumenti normativi già in vigore in Italia che, come la direttiva, impongono l'obbligo di denuncia e/o condivisione di ogni evento di sicurezza che possa impattare sull'erogazione di un servizio considerato "essenziale".

La Direttiva prevede un elevato livello di cooperazione tra i Paesi Membri dell'Unione Europea. Tale cooperazione richiede la presenza sui differenti territori nazionali di specifici **CSIRT** (Computer Security Incident Response Team) collegati tra

loro in conformità con quanto previsto dall'Art. 11 della Direttiva in questione.

Il Gruppo FSI dispone da oltre un anno di un CSIRT in linea con quanto previsto dalla Direttiva e già predisposta per la comunicazione con il CSIRT "Transportation" che verrà a breve introdotto dal **MIT** (Ministero delle infrastrutture e dei trasporti), designato come autorità competente NIS.

Entro novembre 2018 è previsto che il MIT identifichi gli operatori di servizi essenziali per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada e sarà interessante comprendere quale saranno i criteri identificazione.

Il recepimento di tale Direttiva è un importante passo avanti nella realizzazione di un piano di cybersecurity nazionale che prevede la cooperazione e partecipazione tra il pubblico e il privato. È però fondamentale che i tavoli di lavori istituiti abbiano tutte le competenze e le risorse necessarie per garantire la massima efficacia. A tal fine, il Gruppo è parte attiva nel supportare il suddetto tavolo all'elaborazione di questi elementi. Riteniamo che molto lavoro ancora deve essere fatto nella direzione di certificare attraverso enti istituzionali le soluzioni di sicurezza in uso ai cosiddetti "operatori di servizi essenziali". È noto che le attuali leggi sugli appalti pubblici non consento di premettere parametri stringenti di qualità e di indirizzo, sulle acquisizioni da mercato delle soluzioni e delle tecnologie. Dunque ci aspettiamo da parte delle nostre istituzioni iniziative in tal senso, peraltro già in uso in altri Paesi.

The post Infrastrutture critiche, come proteggere quelle nazionali? Intervista a Danilo Gismondi (Trenitalia) e Riccardo Barrile (Gruppo FS) appeared first on Key4biz.

https://www.key4biz.it/infrastrutture-critiche-come-proteggere-quelle-nazionali-intervista-a-danilo-gismondi-trenitalia-e-

riccardo-barrile-gruppo-fs/231672/

Hackerato sito patronato Cisl, online email e telefoni di 37mila persone

Indirizzo e-mail, password e, dove indicati, numero di telefono e professione delle 37.500 persone iscritte al sito web del **Patronato Inas-Cisl** sono adesso alla mercé di tutti. Sono stati pubblicati online dopo l'attacco informatico, conclusosi con successo, al *"database relativo ai dati inseriti nell'area personale, utilizzata per accedere ad alcuni servizi del Patronato"*, ha annunciato il patronato della Cisl sul sito stesso il 7 settembre: *"L'Istituto sta provvedendo ad attivare tutte le azioni di verifica e tutela dei dati contenuti nel sito Inas"*. Il patronato ha immediatamente segnalato il Data Breach al Garante Privacy, come prevede il **GDPR** si ha 72 ore di tempo per farlo. Lo prevede anche il decreto legislativo per l'adeguamento della normativa nazionale al GDPR, ma il provvedimento entrerà in vigore nel nostro Paese il 19 settembre.
La violazione è stata denunciata anche alla Polizia Postale.

Ma chi è stato l'autore dell'attacco hacker al sito del patronato della Cisl?

È stato rivendicato da **LulzSecItalia.**

> *Sorprende quanto a @InasCisl importi ben poco dei #dati #sensibili che tratta. Mettendo così in serio pericolo le vite delle 37.500 persone, di cui sono stati diffusi i dati*

> *personali ieri. #FacciamoChiarezza #LulzSecITA #Hacked #INAS #Anonymous #GDPR @arturodicorinto*
>
> *— LulzSecITA (@LulzSec_ITA) 7 settembre 2018*

La nota del sito del patronato della Cisl

I dati sottratti sono unicamente quelli anagrafici e quelli di registrazione degli utenti al sito (indirizzo e-mail, password e, ove indicati, numero di telefono e professione). Ci preme sottolineare che i dati relativi alle pratiche aperte presso le nostre sedi non sono conservati sul database del nostro sito web e non sono quindi stati oggetto della violazione.

La violazione è stata immediatamente denunciata al Garante per la Privacy e alla Polizia Postale e sono in corso verifiche approfondite per riportare il sistema alla normale operatività.

Siamo consapevoli del fatto che questo incidente causa disagi ai nostri utenti: li stiamo contattando tutti per scusarci dell'inconveniente e continueremo a tenerli informati nei prossimi giorni attraverso questa pagina.

The post Hackerato sito patronato Cisl, online email e telefoni di 37mila persone appeared first on Key4biz.

https://www.key4biz.it/hackerato-sito-patronato-cisl-online-email-e-telefoni-di-37mila-persone/231222/

Cybertech 2018, anche Accenture alle kermesse del 26 e 27 settembre a Roma

Nel corso dell'ultimo anno ci sono state numerose discussioni e dibattiti, nonché preoccupazione, intorno al tema della sicurezza informatica e del **GDPR**. Temi che riguardano tutti, imprese e singoli individui. Se parliamo di cyber security non ci si può fermare: cultura e innovazione devono andare di pari passo ed evolversi per poter far fronte alle continue minacce informatiche.

Per il terzo anno consecutivo, la conferenza annuale Cybertech Europe si terrà dal 26 al 27 settembre a Roma. Una opportunità unica per tutti i visitatori per conoscere le ultime innovazioni, incontrare potenziali clienti e gettare lo sguardo sul futuro di questo settore.

È quanto mai fondamentale adottare un approccio vigile per salvaguardarsi da possibili rischi futuri e minacce sconosciute. Ogni azienda, piccola o grande che sia, deve dotarsi di strumenti in grado di prevedere, rilevare e affrontare adeguatamente le minacce.

Cybertech Europe, punto di incontro tra tutti i leader di settore ed esperti provenienti da tutto il mondo, sarà l'occasione per comprendere meglio il panorama attuale e i risvolti futuri del mercato globale della cyber security. Lo scambio di idee e la collaborazione tra gli attori coinvolti rappresentano il punto di forza per aprire la strada a un

livello successivo di prevenzione.

Durante l'evento una grande sala espositiva sarà il teatro di aziende e PMI protagoniste di tutto il mondo, mentre il **Global Cybertech Startup Pavilion** ospiterà startup innovative che metteranno in mostra le loro tecnologie più all'avanguardia.

"Il tema della cyber security non è in cima alle priorità nelle agende e capita sempre più spesso che sia trattato in modo marginale nel contesto tecnologico, quando, in realtà, è fondamentale in tutti i settori verticali, indistintamente che si tratti di hardware o software, e ha – in ultima analisi – un impatto sulla vita quotidiana", sostiene **Amir Rapaport**, fondatore e editor in chief di Cybertech. *"Abbiamo ideato Cybertech per diffondere consapevolezza su questi temi e dimostrare come tutte le imprese, indipendentemente dalle loro dimensioni o dai target – startup, grandi aziende o enti pubblici – debbano adottare un approccio proattivo se vogliono gestire e affrontare in modo efficace le minacce informatiche, rimanendo al contempo competitive, innovative e di successo".*

"Come ben sappiamo, minacce e attacchi a livello informatico possono provenire da diversi Paesi e diffondersi molto rapidamente, superando barriere e confini. Per questo, quello della cyber security è un tema di portata globale e le sfide ad esso connesse possono essere affrontate solo attraverso la condivisione e la collaborazione, riunendo allo stesso tavolo una community di competenze ed esperienze internazionali", commenta **Alessandro Profumo**, Amministratore Delegato di Leonardo. *"Giunto alla sua terza edizione, Cybertech Europe 2018 vedrà Leonardo rafforzare il suo impegno nel sostenere sempre il dibattito su questi temi a livello paneuropeo e internazionale. Si tratterà anche di promuovere la*

digitalizzazione, che non è meramente un pretesto per cybercriminali o malintenzionati, ma piuttosto un punto di forza che può portare al progresso sociale ed economico".

Cybertech Europe 2018, iniziativa promossa da Cybertech Global Events e Leonardo, si terrà dal 26 al 27 settembre presso il **Convention Center La Nuvola di Roma**.

Giornalisti e rappresentanti del Governo possono registrarsi gratuitamente al seguente link: inoltre sono disponibili tariffe scontate per gli studenti.

Per registrarti all'evento, clicca qui.

The post Cybertech 2018, anche Accenture alle kermesse del 26 e 27 settembre a Roma appeared first on Key4biz.

https://www.key4biz.it/cybertech-2018-anche-accenture-alle-kermesse-del-26-e-27-settembre-a-roma/230977/

Allarme del WEF, l'AI porterà al collasso la finanza globale?

L'Intelligenza Artificiale porterà al collasso il sistema finanziario globale? L'allarme arriva dal **World Economic Forum (WEF),** che in un report recente sulle trasformazioni legate all'avvento dell'AI mette in guardia dal rischio di una crisi globale che potrebbe scoppiare prima ancora che ce ne rendiamo

conto.

Il problema, secondo il report del WEF, sta nel modo in cui i mercati finanziari globali stanno adottando e implementando le nuove tecnologie di machine learning e AI.

"Le nuove dinamiche di machine learning creano un forte incentivo alla digitalizzazione del back office – si legge nel report realizzato da **Jesse McWaters**, responsabile AI dei Financial Services Project del WEF – *Un mondo più connesso e reticolare è più vulnerabile al rischio cybersecurity e inoltre crea maggiori rischi di concentrazione dei network".*

In parole povere, il sistema fiannziario sta sì implementando una rete con meno punti di accesso a rischio di attacchi cibernetici, ma così facendo rende il network globale più vulnerabile ad eventuali attacchi che potrebbero mettere in ginocchio l'intero sistema dei mercati.

Mentre i servizi decentralizzati basati sulla blockchian, come il bitcoin, sono fondati sulla condivisione di dati decentralizzati, banche e istituzioni finanziarie globali stanno realizzando sempre più prodotti basati su AI e machine learning che risidedono sul cloud.

Un trend in grande crescita, che coinvolge ormai migliaia di banche e istituti finanziari, che sfruttano tutti lo stesso metodo di accesso attraverso gli stessi strumenti, vale a dire un punto centrale di accesso a tutti i servizi conservati in cloud, che rappresenta un target molto appettibile per i cybercriminali. Senza considerare che l'intero sistema potrebbe un giorno o l'altro crollare sotto il peso di se stesso.

Un rischio già ventialto nel 2013 da **Andrew Lo**, professore alla Sloan School of Management del MIT, che mise in guardai appunto dal pericolo che un sistema così congegnato potrebbe semplicemente collassare prima o poi, come un castello di carte, sotto il peso della sua complessità. *"Eventuali choc ad*

un singolo nodo dell'enorme network globale di computer, reti di telecomunicazioni e potenza di calcolo potrebbero propagarsi facilmente e in maniera rapida e imprevedibile ad altre parti del network", ha detto Lo.

Il tutto senza considerare un altro aspetto preso in considerazione dal WEF, vale a dire la crescente fragilità delle tech company. Il WEF solleva dubbi sull'ingresso delle grandi tech company sul mercato dei servizi finanziari, con il conseguente rischio di un rapporto simbiotico e dannoso per il mercato con le grandi aziende del settore Finance. Un allarme confermato dai fatti, visto il caso appena esploso sull'accordo segreto sotto la lente del anche del Garante Privacy fra **Google** e **Mstercard** per lo sfruttamento indebito dei dati di acquisto di 2 miliardi di clienti americani del colosso delle carte di credito a scopi commerciali senza consenso.

The post Allarme del WEF, l'AI porterà al collasso la finanza globale? appeared first on Key4biz.

https://www.key4biz.it/allarme-del-wef-lai-portera-al-collasso-la-finanza-globale/230594/

Cybercrime, perso 1 milione di dollari ogni minuto

Globalmente, ogni minuto vengono persi più di 1,138,888 milioni di dollari a causa del crimine informatico,con un aumento rispetto all'anno scorso di 282.724 dollari. A rivelarlo è la società di sicurezza informatica americana **RiskIQ** nel nuovo report **'Evil Internet Minute 2.0'.**

Il report evidenzia come ogni 60 secondi 1.861 persone sono colpite da attacchi informatici come malware e phishing. E non c’è da meravigliarsi se così tante persone sono vittime di crimini: ogni minuto, hacker da tutto il mondo distribuiscono collettivamente 1.274 malware, 22.9 e-mail phishing, 9 annunci pubblicitari fake e 21 nuovi domini di phishing.

Il report di RiskIQ spiega che le aziende spendono collettivamente 171,233 dollari al minuto sulla sicurezza IT, ma questo non basta. Ogni 60 secondi, 1.5 organizzazioni sono vittime di attacchi ransomware. Questi attacchi collettivamente costano alle aziende in media più di 15,221 dollari al minuto.

Anche l’impatto delle violazioni dei dati è sbalorditivo. Ogni giorno vengono rubate 2,9 miliardi di informazioni e divulgate pubblicamente.

The post Cybercrime, perso 1 milione di dollari ogni minuto appeared first on Key4biz.

https://www.key4biz.it/cybercrime-perso-1-milione-di-dollari-ogni-minuto/229951/

Microsoft, tra politica e mossa commerciale ‘La mano di Mosca sulle elezioni USA di novembre. Al sicuro con il nostro software anti-hacker’

“È chiaro che le democrazie di tutto il mondo sono sotto attacco. Le entità straniere stanno lanciando attacchi informatici per influenzare le elezioni e seminare discordia”. Inizia così il post in cui il presidente di **Microsoft**, **Brad Smith**, lancia l’allarme hacker russo pronto ad influenzare di nuovo un voto elettorale in Occidente, dopo i tentativi di interferire (ancora non si sa con quale risultato) nelle presidenziali Usa del 2016 e in quelle francesi del 2017, e chissà anche nelle elezioni politiche italiane del 4 marzo scorso.

Quindi Smith (e la compagnia di Bill Gates) fa politica dopo aver assunto i panni di scheriffo: *“La scorsa settimana, la Digital Crimes Unit (DCU) di Microsoft ha eseguito con successo un’ingiunzione del tribunale per interrompere e trasferire il controllo di sei domini internet creati da un gruppo ampiamente associato al governo russo e noto come Strontium, o in alternativa Fancy Bear o APT28. Abbiamo*

bloccato questi attacchi 12 volte in due anni e chiuso 84 siti Web fake associati a questo gruppo”.

Qual era l’obiettivo degli hacker russi secondo Microsoft? I domini tentavano di spacciarsi per il Senato Usa e per due organizzazioni conservatrici americane, l’Hudson Institute e l’International Republican Institute. Una volta che si cliccava su questi siti si veniva reindirizzati a pagine che tentavano di rubare le password degli utenti.

Il fine dell’interferenza russa, in vista delle elezioni di medio termine di novembre, sarebbe stato quello di contrastare la tendenza dei gruppi repubblicani moderati o tradizionali, ostili a Trump e favorevoli a perpetuare le sanzioni alla Russia.

Da Microsoft anche una mossa commerciale?

Dopo aver lanciato l’allarme delle democrazie sotto attacco dagli hacker russi, il presidente di Microsoft ha presentato la nuova soluzione della società per la sicurezza informatica,

messa a disposizione, gratuitamente, per tutti i candidati e gli uffici elettorali fino ai think tank e ai partiti *“che ora crediamo siano sotto attacco”.* Il software è gratuito, ma solo per chi utilizza Office 365, che è a pagamento, salvo nella versione educational.

Dunque l’allarme lanciato da Microsoft è sentito o è una trovata di marketing? Perché ricorda la mossa commerciale adottata da **Apple** nelle indagini sulla strage di San Bernardino avvenuta in California nel 2015. La società di Cupertino si è rifiutata di aiutare l’FBI a sbloccare l’iPhone 5C di uno dei due attentatori, mandando così, in modo sottointeso, un forte messaggio commerciale veicolato in tutto il mondo: *“neanche l’FBI riesce a sbloccare i nostri smartphone”* oppure *“difendiamo sempre la privacy dei nostri clienti, di fronte alla richiesta di qualsiasi Governo”.*

The post Microsoft, tra politica e mossa commerciale ‘La mano di Mosca sulle elezioni USA di novembre. Al sicuro con il nostro software anti-hacker’ appeared first on Key4biz.

https://www.key4biz.it/microsoft-tra-politica-e-mossa-commerciale-la-mano-di-mosca-sulle-elezioni-usa-di-novembre-al-sicuro-con-il-nostro-software-anti-hacker/229756/

Il malware non va in vacanza, l’Adware è la nuova minaccia per gli italiani

Le minacce informatiche non vanno in vacanza, soprattutto in estate quando migliaia di utenti distratti dalle ferie e dai momenti di relax, compiono inconsapevolmente azioni che

possono compromettere la sicurezza dei propri device. Secondo la speciale classifica condotta da **ESET** sulla sicurezza informatica, l'estate 2018 vede il ritorno degli adware, software che durante la navigazione su Internet raccolgono informazioni sulle operazioni effettuate dall'utente, che visualizza periodicamente annunci pubblicitari non richiesti.

La classifica

Svetta infatti al primo posto della classifica, con il 12% delle rilevazioni, ***Win32/Adware.Agent.AA*** che, una volta installato sul sistema, diventa la principale causa per la visualizzazione di contenuti promozionali, tra cui pop-up, banner, link di testo e annunci commerciali, che vengono utilizzati per aumentare la popolarità di siti di terze parti. Adware.Agent.AA è inoltre in grado di raccogliere dati sensibili, come le credenziali di accesso all'Internet Banking, che vengono poi usati per finalità fraudolente.

Con **l'8%** di prevalenza scende al secondo posto nella classifica ***Js/CoinMiner***, un temibile JavaScript che si diffonde attraverso i contenuti Java infetti, inseriti molto spesso in banner presenti su siti "affidabili" o all'interno di email di phishing contenenti link a pagine pericolose che ospitano questo script. Una volta eseguito nel sistema, CoinMiner installa un trojan creato per generare valuta digitale (attività di *mining*) sfruttando le risorse del sistema infettato. CoinMiner ha raggiunto in Italia il picco di infezioni lo scorso gennaio, toccando l'apice del 32% delle rilevazioni. Da allora questo malware ha iniziato una parabola discendente, toccando il suo minimo proprio a luglio. I livelli di infezione di CoinMiner rimangono invece ancora alti in alcune nazioni come l'Ucraina (15% delle rilevazioni), l'Ungheria (14%) e la Spagna (11%).

Il terzo posto della classifica delle principali minacce registrate in Italia a luglio 2018 da ESET si posiziona **con il 2% delle rilevazioni *JS/Redirector***, un trojan che reindirizza il browser a una URL specifica contenente un software dannoso. Il codice del programma del malware è solitamente incorporato nelle pagine HTML. Il picco massimo di infezioni da Redirector si è registrato a luglio in Polonia, con il 6% delle rilevazioni.

Al quarto e al quinto posto della classifica troviamo rispettivamente ***Win32/Exploit.CVE-2017-11882*** (1,80% delle rilevazioni) e ***Win32/GenKryptik*** (1,50% delle rilevazioni)***.*** Il primo sfrutta una vulnerabilità – aggiornata da Microsoft a luglio 2017 – per l'esecuzione di codice da remoto in Microsoft Office, mentre il secondo è una segnalazione euristica di ESET di una minaccia ancora non completamente identificata.

Non solo Adware, boom dei Trojan bancari

Un'ondata significativa di minacce informatiche spetta ai Trojan bancari, uno dei più pericolosi tipi di malware, progettati per rubare denaro direttamente dai conti correnti degli utenti in ambito mobile. Nel secondo trimestre del 2018 hanno raggiunto le 61.045 unità secondo gli analisti di Kaspersky Lab.

Questo tipo di attacco è di grande interesse per i criminali informatici di tutto il mondo, alla costante ricerca di

guadagni facili. Di solito il malware ha le sembianze di una app legittima, per indurre le persone ad installarla. Una volta avviata l'applicazione bancaria, il Trojan mostra la propria interfaccia sovrapponendola all'interfaccia della app di mobile banking. Quando l'utente inserisce le proprie credenziali, il malware procede con il furto delle informazioni.

Nel secondo trimestre del 2018, i primi tre paesi con la quota più consistente di utenti attaccati con malware bancari per dispositivi mobile – in percentuale rispetto al numero relativo a tutti gli utenti colpiti da un qualunque altro tipo di malware – sono stati U.S.A. (0,79%), Russia (0,7%) e Polonia (0,28%). Russia e U.S.A. si sono scambiate la posizione in classifica rispetto al primo trimestre del 2018, mentre la Polonia è passata dal 9° al 3° posto; la causa principale di questo passaggio alla top 3 è stata la distribuzione attiva di minacce come Trojan.AndroidOS.Agent.cw e Trojan-Banker.AndroidOS.Marcher.w.

Secondo gli esperti, numeri così alti potrebbero essere parte di una tendenza globale, caratterizzata dalla crescita di malware rivolti al mondo mobile: il numero complessivo di pacchetti di installazione di malware per mobile è aumentato di oltre 421.000 unità nel secondo trimestre del 2018 rispetto al trimestre precedente.

The post Il malware non va in vacanza, l'Adware è la nuova minaccia per gli italiani appeared first on Key4biz.

https://www.key4biz.it/il-malware-non-va-in-vacanza-ladware-e-la-nuova-minaccia-per-gli-italiani/229574/

How to Protect Your Personal Brand’s Website From a Cyber Attack

Here are several ways you can effectively protect your website and online reputation. https://www.entrepreneur.com/article/318120

The Latest Thing You Need to Worry About Cybercriminals Hacking? Your Voice.

The shift to voice biometrics and speech-controlled systems is raising the risk of voice cloning and subliminal attacks. https://www.entrepreneur.com/article/318238

WhatsApp supera il miliardo di gruppi attivi, ma pieni di fake news e truffe

È una delle piattaforme di *instant messaging* (IM) più famosa e frequentata al mondo, ora di nuovo al centro di storie di false notizie e raggiri finanziari. Attualmente, ***WhatsApp***, che

è di proprietà di Facebook, conta più di **1,5 miliardi di utenti**, oltre **1 miliardo di gruppi** e **65 miliardi di messaggi inviati ogni giorno**.

In una recente indagine di *cybersecurity*, è saltata fuori una nuova falla che "*permetterebbe a un criminale informatico di intercettare e manipolare i messaggi inviati all'interno dei gruppi di discussione o delle chat private*".

Gli hacker, quindi, potrebbero a detta dei ricercatori sfruttare questa vulnerabilità "*non solo dirottando la conversazione a loro vantaggio, ma anche creando e diffondendo fake news*".

Le conseguenze della vulnerabilità possono essere diverse e comportare altrettante azioni da parte dei cyber criminali, tra cui: **sostituire la vera risposta di un utente con un'altra** puramente inventata; citare un messaggio mentre si risponde in un gruppo così da farlo apparire come se provenisse da una persona che non fa nemmeno parte del gruppo; inviare un messaggio a un membro di un gruppo, sotto forma di un messaggio di gruppo, ma che di fatto viene inviato solo a un destinatario.

Le conseguenze reali?

Il criminale manipola il testo di una risposta così da fornirne una che potrebbe essere di grande beneficio per lui. Oppure, **i criminali informatici potrebbero diffondere informazioni errate su un determinato prodotto e causare così gravi danni anche d'immagine a un'azienda.**

Gli hacker, infine, potrebbero **trarre in inganno i membri di un gruppo inducendoli a svelare segreti di qualsiasi tipo e**

informazioni riservate a loro insaputa.

Altra vulnerabilità, stavolta scoperta da Eset, riguarda la **cyber sicurezza** generale della piattaforma, con il rischio concreto per molti degli iscritti della piattaforma di IM di aprire messaggi truffa finalizzati, come sempre, al sottrarre risorse finanziarie alle sfortunate vittime.

Con il messaggio ambiguo e falso di "*insegnare a clonare gli account degli altri utenti e vedere il contenuto dei messaggi che mandano e ricevono*", la vittima spinta dalla curiosità risponde a tutti gli *imput* fino a quando finisce per attivare, probabilmente inconsapevolmente, un **servizio SMS a pagamento che consuma il credito dello smartphone**.

Facendo leva non solo sulla curiosità, ma soprattutto su altri sentimenti più forti, come gelosia e invidia, i cyber criminali fanno cadere l'utente nel tranello e allo stesso tempo lo obbligano a condividere il messaggio delle finte istruzioni per clonare un account con tutti i suoi contatti, favorendo in definitiva la diffusione del malware.

Ogni SMS ci può scalare fino a 5 dollari dal credito e ne possono partire più di uno contemporaneamente.

The post WhatsApp supera il miliardo di gruppi attivi, ma pieni di fake news e truffe appeared first on Key4biz.

https://www.key4biz.it/whatsapp-supera-il-miliardo-di-gruppi-attivi-ma-pieni-di-fake-news-e-truffe/229324/