WannaCry, tre anni dopo la Corea del Nord ci riprova con nuovi malware

Questa settimana i funzionari della sicurezza informatica degli Stati Uniti hanno pubblicato dettagli su tre varietà di malware che sono state utilizzate dagli hacker sponsorizzati dal governo della **Corea del Nord** per attaccare obiettivi in tutto il mondo.

L'annuncio, secondo quanto riporta ZDNet, coincide con il terzo anniversario dell'epidemia di ransomware **WannaCry**, l'ondata di attacchi informatici di tipo ransomware che ha mandato in tilt i pc e i dispositivi elettronici di mezzo mondo nel maggio del 2017.

Un attacco su vasta scala, denominato ***WannaCry***, mirato a sequestrare letteralmente i computer, con l'obiettivo di chiedere un riscatto, molto spesso inutilmente pagato dalle vittime.

I funzionari statunitensi, che hanno incolpato il regime di Pyongyang, hanno indivuato i seguenti tre ceppi di malware:

- **Copperhedge**

Si tratta di un trojan di accesso remoto (RAT) in grado di eseguire comandi arbitrari, ricognizioni del sistema ed rubare dati. Sono state identificate sei diverse varianti.

- **Taintedscribe**

Un malware (trojan) installato su sistemi compromessi per ricevere ed eseguire i comandi dell'attaccante. Questi esempi

usano FakeTLS per l’autenticazione della sessione e per la crittografia di rete utilizzando un algoritmo LFSR (Linear Feedback Shift Register).

- **Pebbledash**

Questo malware ha la capacità di scaricare, caricare, eliminare ed eseguire file; abilitare l’accesso alla CLI di Windows; creare e terminare processi; ed eseguire l’enumerazione del sistema di destinazione.

Il gruppo criminal hacker Hidden Cobra

Le informazioni circolanti, contenute in diversi documenti noti come report di analisi dei malware (MAR), descrivono in dettaglio l’attività degli hacker di **Hidden Cobra**, un gruppo avanzato di minacce persistenti che il governo degli Stati Uniti ha precedentemente collegato al governo nordcoreano.

Il gruppo Hidden Cobra si rivolge spesso a istituzioni finanziarie come banche, scambi di criptovaluta e sportelli automatici per ottenere guadagni finanziari, afferma il governo Usa. Tuttavia, non è stato immediatamente chiaro quali specifici incidenti di sicurezza, se presenti, il governo degli Stati Uniti ha cercato di esporre nello sforzo di condivisione delle informazioni.

https://www.key4biz.it/wannacry-tre-anni-dopo-la-corea-del-nord-ci-riprova-con-nuovi-malware/305778/

Sicurezza Nazionale, addio CERT-PA. Dal 6 maggio via al CSIRT Italia

Al via dal prossimo 6 maggio il trasferimento delle funzioni del **CERT-PA** e il **CERT Nazionale** allo **CSIRT Italia**, il nuovo team per gestire la cyber-difesa nazionale italiana istituito presso il Dipartimento Informazioni per la Sicurezza (**DIS**).

CSIRT Italia

Lo ha annunciato in una nota lo stesso CERT-PA in cui spiega come entrambe le strutture, che sino ad oggi hanno rispettivamente supportato le pubbliche amministrazioni e il settore privato nella prevenzione e nella risposta agli incidenti informatici, termineranno tutti i servizi proattivi e reattivi.

Entrambe passeranno con gradualità le consegne dal 6 maggio, da tale data, inoltre, i due CERT cesseranno contestualmente di esistere come soggetti autonomi.

La direttiva NIS

La decisione rientra nell'ambito del piano di attuazione della Direttiva NIS (Decreto legislativo 18 maggio 2018 n. 65), recante le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea, che – tra le altre misure – prevede anche in Italia la costituzione di un **Computer Security Incident Response Team unico** (cosiddetto CSIRT).

L’attività dello CSIRT è disciplinata dal DPCM 8 agosto 2019 in materia di “*Disposizioni sull’organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano*”, pubblicato in Gazzetta Ufficiale l’8 novembre 2019.

In tale quadro, i soggetti pubblici e privati, a partire dalla data menzionata, in caso di incidente cibernetico e/o di segnalazione di evento, avranno quale nuovo ed unico interlocutore lo CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli operatori di servizi essenziali (cosiddetti OSE) e Fornitori di Servizi Digitali (cosiddetti FSD) ai sensi della Direttiva NIS.

I compiti del CSIRT

Il CSIRT è istituito presso il **Dis**, il Dipartimento delle informazioni per la Sicurezza, e ha il compito di:

- definire le procedure tecniche per la prevenzione e la gestione degli incidenti informativi
- ricevere le notifiche sugli incidenti, fornire a chi ha effettuato la notifica le informazioni per facilitare una gestione efficace dell’evento ed informare gli altri Stati dell’Ue eventualmente coinvolti.
- Garantire la collaborazione nella rete Csirt, attraverso l’individuazione di forme di cooperazione appropriate, lo scambio di informazioni.

“*Viene così a comporsi un altro tassello importante dell’architettura nazionale cyber* – aveva sottolineato il Dipartimento delle Informazioni per la Sicurezza lo scorso novembre – *che, con la collocazione del Csirt presso il Dis, favorirà una più efficace gestione tecnica degli incidenti a livello nazionale e internazionale, grazie alle sinergie garantite dalle altre funzioni già assicurate dal Dipartimento in tale ambito, quali il ‘punto di contatto unico nazionale Nis’ per la gestione operativa di incidenti transfrontalieri,*

il ‘Nucleo per la Sicurezza Cibernetica (Nsc)’ per la gestione operativa di incidenti che hanno un impatto sulla sicurezza nazionale, e le attivazioni che deriveranno dal cosiddetto ‘Perimetro di sicurezza nazionale cibernetica’.”

Per lo svolgimento dei propri compiti, il **CSIRT** si avvarrà dell’AgID ai sensi del decreto legislativo NIS.

https://www.key4biz.it/sicurezza-nazionale-addio-cert-pa-dal-6-maggio-via-al-csirt-italia/301290/

Zoom, 500mila account in vendita sul dark web

Le informazioni sugli account appartenenti ad almeno mezzo milione di utenti **Zoom** sono state pubblicate, scambiate e, in alcuni casi, vendute sul dark web.

Secondo quanto riportato dal sito Bleeping Computer, l’archivio è stato identificato ad inizio aprile da **Cyble**, una società di sicurezza informatica che ha scoperto e successivamente acquistato più di 530.000 credenziali Zoom rubate attraverso un forum di hacker.

La tecnica del Credential Stuffing

Cyble ha dichiarato a Bleeping Computer che gli hacker sono stati in grado di ottenere gli indirizzi e-mail, le password, i collegamenti URL e le chiavi host degli utenti Zoom tramite

uno schema di attacchi informatici chiamato "***Credential stuffing***", in cui i dati precedentemente trapelati da un'altra fonte online vengono estratti da aree del dark web e usate per compromettere nuovi account.

È qui che gli hacker utilizzano i dettagli dell'account rubati da hack di altri siti per ottenere l'accesso, poiché le persone spesso riutilizzano le stesse password su più siti.

Account venduti per 0,002 centesimi

Alcuni degli account Zoom venivano offerti gratuitamente, mentre altri per meno di 0,002 centesimi ciascuno "*in modo che gli hacker possano usarli in scherzi e attività criminale,* spiega il sito." Si dice anche che gli hacker offrano account gratuiti per "*acquisire una maggiore reputazione nella comunità degli hacker*".

I conti stessi erano vari, molti dei quali riguardavano indirizzi universitari ma includevano anche conti per società ben note, tra cui **JPMorgan Chase Bank N.A. e Citigroup Inc.**

Le colpe di Zoom

È bene precisare che la vicenda non nasce da un attacco diretto a Zoom, ma si basa sullo sfruttamento di **credenziali** già finite nelle mani sbagliate da tempo. Ci sono però dei modi per fornire una sicurezza maggiore agli utenti, come ad esempio l'introduzione dell'**autenticazione a due fattori.** In questo modo infatti, si aggiungerebbe una barriera all'ingresso contro i cybercriminali.

Zoom e Covid-19

Durante la pandemia **COVID-19**, Zoom è emerso alla ribalta, arrivando in cima ai download delle applicazioni. Con questa popolarità sono anche uscite allo scoperto le sue pratiche di

sicurezza, rivelatesi carenti.

A parte i problemi di sicurezza, Zoom è una delle poche aziende che ha superato bene la pandemia di coronavirus. Il prezzo delle azioni di Zoom ha raggiunto il picco di 159,56 dollari lo scorso 23 marzo, anche se le questioni di sicurezza hanno attenuato leggermente l'interesse degli investitori.

https://www.key4biz.it/zoom-500mila-account-in-vendita-sul-dark-web/300083/

Coronavirus, come difendersi dai principali vettori di attacco hacker

Non è una novità purtroppo, potreste aver già letto di come i **Criminal Hacker** stiano capitalizzando la pandemia di **coronavirus** in corso nel tentativo di infettare i computer e dispositivi mobile con malware o anche solo di portare a termine vari tipi di truffe.

Criminal hacker e Covid-19

Sfortunatamente, in una certa misura, sta funzionando. Questo perché la superficie di attacco sta cambiando e si sta espandendo rapidamente, dato che molte organizzazioni e aziende si stanno digitalizzando senza molta preparazione, esponendosi a più minacce potenziali.

La maggior parte dei recenti Cyber attacchi sfruttano principalmente i timori legati all'epidemia di COVID-19, alimentati dalla disinformazione e dalle false notizie, per distribuire malware tramite le applicazioni **Google Play**, link e allegati dannosi ed eseguire attacchi ransomware.

Nuovo tema, vecchi pericoli

Ogni Paese del mondo ha visto almeno un attacco a tema COVID-19 realizzato ex novo. Questi attacchi rappresentano tuttavia meno del 2% di tutti i Cyber incident solitamente tracciati, secondo un recente studio di **Microsoft**.

I dati raccolti, infatti, mostrano che queste minacce a tema COVID-19 sono una ricostruzione di attacchi esistenti che sono stati leggermente modificati per legarsi a questa pandemia. Ciò significa che stiamo assistendo a un cambiamento delle esche, non ad un'impennata di nuovi strumenti del Cyber Crime.

Ma quali sono i metodi più in voga al momento?

Mobile Malware

I Criminal Hacker stanno sfruttando le paure e i timori delle persone riguardo ai coronavirus per diffondere malware mobile, compresi i Mobile Remote Access Trojans (MRAT), i banker trojans e i dialer premium, tramite app che affermano di offrire informazioni relative al Coronavirus e aiuto per gli utenti.

Solo per citare un esempio, un team di ricerca statunitense, ha recentemente scoperto almeno 16 diverse applicazioni mobili, che sostenevano di offrire informazioni relative all'epidemia ma che invece contenevano malware, tra cui adware (Hiddad) e banker Trojans (Cerberus), che rubavano i dati personali degli utenti o generavano entrate fraudolente da

servizi a tariffa premium.

Tutte le 16 app in questione sono state scoperte su domini correlati al coronavirus di nuova creazione, che hanno visto un enorme aumento nelle ultime settimane.

Phishing

Sempre in voga, adesso più che mai, questo metodo ha trovato un forte alleato nella propagazione delle botnet. La maggior parte delle e-mail di phishing relative a COVOD-19 sono, tra l'altro, unite a malware come AgentTesla (45%), NetWire (30%) e LokiBot (8%) incorporati come allegati, permettendo così all'aggressore di rubare dati personali e finanziari delle vittime.

Le e-mail, molto spesso, sono state mascherate da avvisi dell'Organizzazione Mondiale della Sanità, dell'UNICEF e di altre agenzie e società internazionali come Maersk e CISCO.

Malware as a Service con scontistica dedicata

Contestualmente all'aumento dell'infezione c'è stata anche un'impennata di post su forum underground dove gli utenti offrivano sconti sui malware e codici promozionali su DDoS, spamming e altri servizi malware. Una sorta di solidarietà perversa tra Criminal Hacker

Smishing

È stata anche rilevata un'impennata di falsi messaggi SMS di mittenti come "COVID" e "UKGOV" che contengono un link a siti di phishing. Oltre agli SMS, i canali possibili includono WhatsApp e altri servizi di messaggistica.

Software dannoso

Mentre le persone lavorano sempre più spesso da casa e le piattaforme di comunicazione online come Zoom e Microsoft Teams diventano cruciali, i Criminal Hacker inviano e-mail di

phishing che includono file dannosi con nomi come “zoom-us-us-zoom_##############.exe” e “microsoft-teams_V#mu#mu#D_##############.exe” nel tentativo di ingannare le persone a scaricare malware sui loro dispositivi.

Ransomware

I criminali informatici stanno cercando di colpire i principali ospedali e altre istituzioni in prima linea nella lotta contro COVID-19 con attacchi Ransomware.

I criminali informatici stanno usando il ransomware per tenere in ostaggio gli ospedali e i servizi medici in modo digitale, impedendo loro di accedere a file e sistemi vitali fino a quando il riscatto non sarà pagato. Alcuni casi hanno compreso Paesi come Regno Unito e Repubblica Ceca.

Come difendersi

I Criminal Hacker adattano continuamente le loro tattiche per trarre vantaggio da nuove situazioni, e la pandemia COVID-19 non fa eccezione. Stanno usando l’elevato appetito per le informazioni relative a COVID-19 come un’opportunità per fornire malware e ransomware e per rubare le credenziali degli utenti.

Il consiglio è sempre lo stesso, non abbassare mai la guardia di fronte a tutto ciò che riceviamo via mail o che decidiamo di scaricare.

In generale, evitare di cliccare sui link nelle e-mail non richieste e diffidare degli allegati di posta elettronica, non rendere pubbliche le riunioni e assicurarsi che siano protette da password per evitare il dirottamento delle videoconferenze.

Non dobbiamo mai e poi mai dimenticare: la cura per il COVID-19 non la troveremo mai online!

https://www.key4biz.it/coronavirus-come-difendersi-dai-princip

ali-vettori-di-attacco-hacker/299703/

Sito INPS in down, troppo facile dare la colpa agli hacker

*La rubrica "**Digital & Law**" è curata da **D&L Net** e offre una lettura delle materie dell'innovazione digitale da una prospettiva che sia in grado di offrire piena padronanza degli strumenti e dei diritti digitali, anche ai non addetti ai lavori. Per consultare tutti gli articoli clicca qui.*

Il 1° d'aprile (sembra uno scherzo e, invece, no), il sito **INPS** è andato in palla e, per giunta, chi era riuscito ad accedere ha potuto vedere dati di altri utenti. Sovraccarico e attacchi hacker, ha dichiarato il Presidente **Pasquale Tridico** in interviste al limite del "balbettante".

Subito dopo, si è iniziato a parlare di attacchi anche alle nostre eccellenze della Sanità come l'**Istituto Spallanzani.**

Hacker e sito INPS in down

La colpa viene tendenzialmente attribuita agli "hacker", entità, peraltro, non completamente chiara a tutti quelli che usano il termine.

Al di là di ciò, abbiamo realmente prove della responsabilità di qualche "attaccante informatico"? Nulla si può escludere,

ma, in realtà, la prospettiva dovrebbe essere invertita perché, come vedremo alla fine, certi assunti perentori potrebbero non essere leciti.

Scendiamo nei particolari, usando anche conoscenza di un certo mondo (quello veramente “hacker”) e logica.

I sabotatori non compiono le azioni di disturbo, ma di ricatto

Chi conosce realmente gli hacker sa che i loro scopi sono dimostrativi (denunciare le manchevolezze informatiche di un certo sistema sbandierato come perfetto, ad esempio) oppure politici (sabotaggio di certe politiche ritenute sbagliate). Io, personalmente, non condivido tutto ciò, ma nell’economia di questo scritto posso affermare che il vero “hacker” non compie azioni giusto per rompere le scatole, per un fine malevolo.

D’altro canto, esistono anche altri soggetti appartenenti alla criminalità comune (pur informatizzata) che si attivano in certi momenti esclusivamente per motivi economici. E’ quello che sembra stesse per accadere per lo Spallanzani, dove pare sia emerso un tentativo di estorsione di tipo “***ransomware***” (appunto, programmi ricattatori).

Giusto per parlare di reati, abbiamo appena nominato l’estorsione (“sei mi dati tot **Bitcoin**, ti sblocco i dati che ti ho reso inaccessibili), ma ci sono anche gli accessi abusivi e/o i danneggiamenti di sistemi pubblici o di pubblica utilità.

Le ‘associazioni’ di hacker

Ora, non sono cose che dico io con un semplice “buonsenso”. Basta seguire un qualsiasi TG un po’ più critico che fa approfondimenti senza appiattirsi sulle dichiarazioni

ufficiali.

Il dubbio – a mio modo di vedere legittimo – è che per giustificare inefficienze della macchina pubblica (sotto finanziata, sottopagata, mal gestita, ecc.) si dia la colpa a chi, tutto sommato, non può difendersi, sostanzialmente perché non esiste: non esiste, infatti, un'associazione degli hacker. Quelli un po' più organizzati (**Anonymous**) hanno preso immediatamente le distanze.

L'INPS e la comunicazione

Ma la cosa non finisce qui perché denunciando, peraltro "a reti unificate", reati così gravi (accessi abusivi e/o danneggiamenti a sistemi informatici pubblici o di pubblica utilità o altri abusi di dati – tutti reati perseguibili d'ufficio) si rischia, a propria volta, di commettere un reato, precisamente quello di "Simulazione di reato" previsto dall'articolo 367 c.p. "*Chiunque, con denuncia, querela, richiesta o istanza, anche se anonima o sotto falso nome, diretta all'Autorità giudiziaria o ad un'altra Autorità che a quella abbia obbligo di riferire, afferma falsamente essere avvenuto un reato, ovvero simula le tracce di un reato, in modo che si possa iniziare un procedimento penale per accertarlo, è punito con la reclusione da uno a tre anni*".

Oltre al fatto che in questo caso conclamato di violazione dei dati ("*data breach*") non sarà semplice scaricare la colpa su ipotetici terzi.

Si badi bene, dunque, a dare la colpa agli altri quando, invece, dipende da inefficienze imputabili a titolare di trattamento.

https://www.key4biz.it/sito-inps-in-down-troppo-facile-dare-la-colpa-agli-hacker/298630/

Smart working, 8 consigli su come lavorare in totale sicurezza

Smart working in Italia

A causa dell'attuale crisi sanitaria e sociale da **Coronavirus** che stiamo vivendo, finalmente nel 2020 l'Italia ha scoperto lo smart working.

Fino a questo momento, infatti, il nostro Paese si attestava tra i meno propensi in Europa a sfruttare questa modalità lavorativa: meno del 5% dei lavoratori svolgeva le proprie attività in maniera stabile o occasionale da casa.

Se da un lato però lo smart working permette alle aziende di continuare la business continuity, dall'altro potrebbe offrire ai criminali informatici nuove opportunità per attacchi mirati, che si tratti di e-mail **di phishing o di altre truffe.**

Covid-19 e cybercrime: Italia 4^ al mondo per attacchi

Secondo l'ultima ricerca dei laboratori **Trend Micro**, i cyber criminali stanno utilizzando la pandemia di Covid-19 come argomento per penetrare le difese di aziende e utenti. Nella lista dei Paesi più colpiti, **l'Italia è quarta** a livello globale per spam ricevuto e sesta per numero di file maligni

rilevati.

Ad oggi, secondo la ricerca, le campagne spam sono sono state lo strumento più utilizzato dai cybercriminali (65,7% degli attacchi). A seguire i malware (26,8%), gli URL maligni (7,5%) e altri strumenti come le truffe BEC e i ransomware.

Come difendersi

E allora come difendersi da queste minacce informatiche per non mettere a rischio la business continuity aziendale mentre si lavora da casa? **IBM Italia** ha stilato 8 consigli su come lavorare in tutta sicurezza senza correre rischi. Ecco quali.

1. Portare a casa solo i dispositivi e le informazioni assolutamente necessarie

Non portare a casa tutti i dispositivi dell'ufficio, ma solo i dispositivi e le informazioni essenziali

2. Salvaguardare la vostra rete domestica e comunicare attraverso connessioni sicure

Proteggere con una forte crittografia **WLAN** la propria Rete di casa con una password unica e complessa e aggiornamenti regolari

3. Tenere aggiornato il software su tutti i vostri dispositivi

Il traffico dati passa attraverso lo stesso router che ha collegati molti altri dispositivi, compresi eventuali elettrodomestici intelligenti che potrebbero non avere una protezione aggiornata. Tutti questi sono potenziali punti di accesso per gli hacker; per questo motivo IBM consiglia di effettuare sempre l'aggiornamento automatico di tutti i dispositivi, sia aziendali che personali.

4. Spegnere i dispositivi intelligenti come Alexa e Siri sulla vostra postazione di lavoro da casa e coprire la webcam quando

non la utilizzate

Spegnere gli assistenti vocali, come Alexa e Siri, in quanto ascoltano ciò che viene detto e lo trasmettono al provider. Non si può quindi escludere che queste registrazioni cadano nelle mani sbagliate. Assicurarsi di coprire la webcam sul vostro PC quando non la utilizzate e fate attenzione a ciò che condividete tramite la funzione video.

5. Distinguere l'utilizzo personale con quello aziendale dello stesso dispositivo

Fate una chiara distinzione tra dispositivi e informazioni per uso aziendale e personale e non trasferite alcun dato di lavoro su dispositivi personali. In questo modo si eviterà qualsiasi fuoriuscita involontaria di informazioni. Come effetto collaterale, questo aiuta anche a separare psicologicamente il tempo in cui si è "al lavoro" da quello in cui si è "a casa".

6. Identificare in modo proattivo tutti i partecipanti alle riunioni online

Le teleconferenze e gli strumenti di videoconferenza sono un'ottima alternativa alle riunioni di persona. Allo stesso tempo, però, è più difficile verificare se tutti i partecipanti sono stati effettivamente invitati. È particolarmente facile per le persone non autorizzate che hanno acquisito i dati di accesso alla videoconferenza, intrufolarsi in grandi riunioni online con molti partecipanti. Ecco perché tutti i partecipanti visualizzati nel software della riunione devono identificarsi brevemente, soprattutto se si trattano argomenti delicati e si condividono le presentazioni sullo schermo.

7. Disconnettersi sempre quando si smette di usare i dispositivi

Bloccate sempre lo schermo del PC e dei dispositivi mobili

quando andate in pausa, in modo che non siano accessibili durante la vostra assenza.

8. Diffidare delle e-mail o degli allegati sospetti, soprattutto se non si conoscete il mittente

Soprattutto durante lo *smart-working*, bisogna diffidare delle e-mail sospette in quanto gli studi dimostrano che la probabilità di cadere vittima di intenzioni malevole è particolarmente alta in casa. Inoltre, non lasciatevi mettere sotto pressione dalle e-mail che chiedono un'azione immediata o che fanno riferimento, ad esempio, all'attuale crisi Covid.

https://www.key4biz.it/smart-working-8-consigli-su-come-lavorare-in-totale-sicurezza/298297/

World Backup Day, l'importanza di proteggere i propri dati personali (Video)

Ogni anno il 31 marzo, si celebra la giornata di sensibilizzazione chiamata **World Backup Day.** Una giornata importante perché ci ricorda che perdere dati e informazioni personali è più facile di quanto si creda.

World Backup Day: i numeri

Ogni minuto vengono persi nel mondo 113 telefoni, il 30% degli utenti non ha mai fatto il backup, cioè una copia dei file più

importanti, dai documenti di lavoro alle foto di famiglia.

Ovviamente, la tecnologia stessa ci viene in aiuto e grazie al ***backup*** possiamo prevenire tali drammatici fatti, mettendo al riparo tutto il nostro mondo, che è un mondo fatto di dati.

L'importanza del backup

L'importanza del backup è quanto mai rilevante in un periodo storico in cui si intensificano sempre di più gli attacchi hacker che prendono di mira gli utenti.

[embedded content]
Come quelli condotti con il *ransomware*, un virus che sequestra i dati e chiede un riscatto. Uno dei modi consigliati dagli esperti per uscire indenni da questo tipo di attacchi è proprio avere una copia dei dati e recuperarli dal backup senza dover sottostare alle richieste dei cybercriminali.

Il costo per le aziende

I dati del "***Global Data Protection Index***" dello scorso anno realizzato da **Vanson Bourne** per **Dell Emc** parlano chiaro: nel 2018 un'azienda italiana su cinque ha perso in modo irrecuperabile una parte dei propri dati.

Spesso le aziende pagano il riscatto agli hacker, e l'azienda di cybersecurity Veritas stima che i ransomware generino un introito annuo dell'ordine di 1 miliardo di dollari e le aziende che non effettuano il backup dei loro dati in maniera sistematica permettono ai criminali di mettere a rischio anche la sicurezza delle informazioni sui loro clienti.

https://www.key4biz.it/world-backup-day-limportanza-di-proteggere-i-propri-dati-personali-video/297895/

Finanza, Banca d’Italia e Consob uniti contro il cybercrime

La **Consob** e la **Banca d’Italia** hanno concordato una strategia comune per rafforzare la sicurezza cibernetica del settore finanziario italiano attraverso specifiche misure rivolte alle infrastrutture finanziarie: sistemi di pagamento, controparti centrali, depositari centrali e sedi di negoziazione dei titoli.

L’accordo Consob/Banca d’italia

Riconoscendo il valore derivante da un approccio cooperativo e sinergico, la strategia mira a contrastare le minacce informatiche legate allo sviluppo delle nuove tecnologie e dell’economia digitale, a innalzare la sicurezza degli operatori finanziari e dei servizi digitali offerti a cittadini, imprese e pubblica amministrazione, nonché ad assicurare l’affidabilità del sistema finanziario nel suo complesso.

Il piano d’azione congiunto riguarda diverse aree di intervento: regolamentazione e supervisione, cooperazione pubblico-privato, formazione e sviluppo di consapevolezza sui rischi cibernetici.

Gli strumenti

In particolare, la Consob e la Banca d'Italia utilizzeranno strumenti di valutazione del rischio cyber, già adottati nell'ambito dell'Eurosistema, come le *Cyber Resilience Oversight Expectations for Financial Market Infrastructures* (CROE), metodologia per la supervisione del rischio cyber.

La Banca d'Italia e la Consob svilupperanno inoltre il TIBER-IT, modello per lo svolgimento di test derivato dal framework europeo di *Threat Intelligence-Based Ethical Red Teaming* (TIBER-EU), valutandone l'ambito, le modalità e la tempistica di applicazione alle diverse entità finanziarie, secondo un principio di gradualità che tenga conto del livello di preparazione degli operatori.

https://www.key4biz.it/finanza-banca-ditalia-e-consob-uniti-contro-il-cybercrime/286072/

Guida autonoma e cybersecurity, quali prospettive per il 2020?

Fino a qualche decennio fa sembrava solo un topos della fantascienza, ma oggi le auto a guida autonoma stanno diventando sempre di più una realtà.

Guida autonoma: i leader del mercato

Da **Uber** a **Google** e – ovviamente – **Tesla capitanata** da **Elon Musk** stanno investendo e sperimentando intensamente su queste tecnologie.

Il colosso del Car sharing e l'indiscusso leader nel mercato delle auto elettriche più in chiave di "affiancamento" alla figura del guidatore, mentre Google ha puntato direttamente sulla guida autonoma.

Ma ovviamente, come con ogni nuova tecnologia "disruptive", sono nati molti dubbi sulla sicurezza di questa, soprattutto perché introducendole nei veicoli ha di fatto introdotto un'altra dimensione nella sfera della sicurezza tipica dell'automobile: alla parte di sicurezza attiva e passiva si è aggiunta quella della cybersecurity.

Dall'infrastruttura alla manutenzione, i rischi fisici e Cyber

Naturalmente non è oro tutto ciò che luccica, come ogni dispositivo connesso e dotato di un processore, i rischi i rischi relativi alla cybersecurity sono dietro l'angolo.

La guida autonoma fa affidamento a software e hardware per tracciare i suoi percorsi (*pathfinding*).

Maggiore sarà il numero di questi veicoli sulla strada maggiore sarà la superficie d'attacco a disposizione dei Criminal Hacker, d'altronde come qualsiasi dispositivo interconnesso questi veicoli devono gioco-forza fare affidamento su altri device, server e servizi per funzionare correttamente; tutti potenziali access point se non

correttamente monitorati e difesi da un efficace perimetro di cybersecurity.

Questo è uno dei grandi scogli nell'implementazione di questi veicoli: presa singolarmente la tecnologia funziona, ma il contesto dove deve operare è tutt'altro che pronto.

Quando all'inizio del secolo scorso le automobili hanno cominciato a diffondersi le strade non erano pronte né tantomeno adeguate ad accoglierle, allo stesso modo oggi le Smart car sono pronte (o quasi), ma l'infrastruttura necessaria a supportarle non è ancora matura.

Guida autonoma: l'impatto della cybersecurity

Questo impatta sia il lato strettamente operativo che quello della cybersecurity. Operativamente la guida autonoma richiederà sempre più massicciamente infrastrutture di rete più affidabili, con fortissimi requisiti di ridondanza e abilità di operare in Real time a seconda delle necessità, nonché una copertura totale del territorio.

Le auto senza conducente hanno già sistemi incredibilmente sofisticati, tra cui computer ad alte prestazioni e un numero crescente di sensori **ADAS** (Advanced Driver Assistance System) come telecamere ad alta risoluzione, **RADAR** e **LIDAR**, nonché grandi schermi 4K/8K e i display head-up (HUD).

Questi sistemi genereranno enormi quantità di dati, che richiederanno un supporto fisico sofisticato: da Data node ad alta velocità a cavi e collegamenti…

È stato stimato che le prossime generazioni di queste vetture arriveranno a inviare 25 gigabyte di dati al cloud ogni ora. Tale mole di dati, ovviamente, comprende anche una grandissima quantità di informazioni sensibili come itinerari di viaggio, storio dei luoghi visitati.

Mantenere intatto questo patrimonio e proteggerlo adeguatamente sarà – a livello di privacy e *Data Integrity* – una delle prime sfide da affrontare per le case automobilistiche e i provider che stanno testando queste tecnologie.

Un'ulteriore area potenzialmente critica è legata alla sicurezza di tutti i sensori che controllano l'area di *obstacle avoidance,* ovvero quelli che analizzano la strada e l'ambiente circostante per reagire a possibili ostacoli o situazioni di emergenza.

Questi lavorano in base a degli algoritmi e sono programmati per rispondere a un vastissimo ventaglio di situazioni, ma cosa potrebbe accadere se l'algoritmo – non sufficientemente protetto e salvaguardato dal punto di vista del suo cybersecurity Framework – venisse corrotto da un Criminal Hacker per non rispondere a pericoli incombenti sulla strada?

Come se non bastasse c'è un ulteriore grandissimo punto di domanda che riguarda il discorso aggiornamenti, croce (per i cybersecurity Provider) e delizia (per i Criminal Hacker) dell'ambito cybersecurity.

Ovviamente per strumenti così innervati di tecnologie l'aggiornamento dei firmware diventa assolutamente critico, allo stesso livello della manutenzione che al momento svolgiamo per la nostra auto.

Ma questo non deve limitarsi alla sola auto a guida autonoma, tutta l'infrastruttura di supporto deve essere costantemente aggiornata; ogni singolo server, ogni singolo endpoint. Un compito sicuramente impegnativo.

Anche lato user finale dobbiamo tenere in considerazione quanto potrebbe impattare la scarsa awerness nei confronti dei Cyber rischi.

Dobbiamo tenere presente che forse solo adesso ha cominciato a

fare breccia nella coscienza comune che per utilizzare pc e smartphone e mantenere sicuri i propri dati ci sia bisogno di un certo livello di consapevolezza; l'introduzione delle auto a guida autonoma potrebbe rimandarci all'anno 0 da questo punto di vista.

Quante volte è capitato che le case produttrici ordinassero un recall di un certo modello per correggere un possibile difetto e venissero ignorate (anche solo da un piccolo substrato dei propri clienti)? Nel caso delle Auto a guida autonoma questa negligenza potrebbe avere conseguenze ben più gravi, come tra l'altro hanno avuto già modo di dimostrare negli Stati Uniti.

I precedenti

Come accennato sono già stati fatti test e ricerche su quanto sia compromettibile e quale sia il livello di controllo che può estrapolare un eventuale attaccante che ottiene accesso ai sistemi informatici di un'auto.

Nel 2017 due ricercatori di un'università americana erano riusciti a dimostrare come fosse facilmente possibile dirottare e prendere il controllo dei veicoli di alcuni famosi brand come Jeep, Ford e Toyota – veicoli "tradizionali" e non certo con il livello di digitalizzazione che possiedono i prototipi di veicoli a guida autonoma.

Nonostante questo erano riusciti a fermare completamente l'auto in marcia sfruttando una vulnerabilità del sistema di infotainment per accedere al CAN-BUS.

Nel mondo reale questo significa che potenzialmente un *threat actor* potrebbe anche arrivare a dirottare il veicolo o costringerlo a girare o frenare all'improvviso per causare disordini o peggio.

Se le auto di oggi sono "semi connesse" e possono essere già così impattate è facile comprendere come le preoccupazioni per

un veicolo a guida autonoma che è completamente basato sul principio dell'interconnessione e con una superfice d'attacco così ampia.

Errare è umano

Forse più che un'problema di immaturità tecnologica dell' "auto senza conducente" stiamo sottovalutando le necessità infrastrutturali che questa richiede sia dal punto di vista fisico che Cyber.

Ciononostante, non si può negare che il mondo ha disperatamente bisogno di ridurre la percentuale di errore che l'uomo commette alla guida. Non stiamo solo parlando degli incidenti stradali, ma banalmente anche di ingorghi e di code.

Facendo un parallelo con il mondo dell'aviazione (caso Boeing escluso) è innegabile come l'automazione dei controlli e l'ingresso di tecnologie come i *glass cockpit* e i sistemi di pilota automatico sempre più avanzati hanno aumentato di *n* volte la sicurezza del trasporto su ala. Non sono semplici speculazioni, i ricercatori del Dipartimento dei Trasporti degli Stati Uniti hanno stimato che le auto a guida autonoma potrebbero ridurre le fatalità dovute agli incidenti sulla strada fino al 94%.

Intervenire a monte

Con miliardi di euro di investimenti in questi progetti da parte di aziende grandi e piccole è abbastanza sicuro che abbiamo da tempo superato il punto di non ritorno, questi mezzi saranno tra poco tra noi.

Prima che l'Uber e la Tesla di turno riescano però a realizzare il loro sogno di flotte di auto autonome c'è la necessità di assicurarsi che tutto il comparto sia allineato sulle necessità di rafforzare il Framework di cybersecurity.

Al momento questa necessità sembra ancora latere, basti pensare che anche la semplice porta ODB – usata universalmente da tutti i meccanici per inserire i loro strumenti di diagnostica – è vulnerabile sia ad attacchi fisici che Cyber.

Citando quanto detto da uno dei ricercatori che ha effettuato i testi sulla Cyber Resilience delle auto: "*I veicoli autonomi sono all'apice di tutte le cose terribili che potrebbero andare male con la tecnologia*".

Un'esagerazione forse, ma come con tutte le tecnologie, dopo una fase di "grazia" dobbiamo fare i conti con i compromessi.

Quali rischi

Le auto autonome hanno buone probabilità di "salvarci" da alcune delle nostre peggiori abitudini. Ma prima di poterlo fare, gruppi privati e pubblici devono sviluppare standard di sicurezza informatica solidi per il settore automobilistico, al contrario c'è il rischio che queste diventino un'arma a doppio taglio e un rischio concreto non solo per la sicurezza dei nostri dati personali, ma anche per la nostra incolumità fisica.

Esistono già dei *must have* imprescindibili per fare fronte alle future minacce: dall'imporre aggiornamenti di firmware tempestivi e obbligatori al taylorizzare i framework in base alla classe e tipologia di veicolo (basti pesare alla differenza oggettiva tra un tir e una semplice auto anche solo in termini di danno potenziale) oltre alla necessità di implementare un protocollo sicuro di comunicazione tra veicolo e veicolo e tra veicolo e infrastrutture e/o device.

Lo scetticismo nei confronti delle nuove tecnologie è giusto. Ma nel caso delle auto senza conducente, a patto di riuscire a costruire un framework di sicurezza solido, potremmo essere davanti a un vero e proprio stravolgimento – in positivo – di come pensiamo e viviamo il trasporto personale.

https://www.key4biz.it/guida-autonoma-e-cybersecurity-quali-prospettive-per-il-2020/284734/

Your Identity Could Be Used in Online Dating Scams. Here's How to Protect Yourself.

Be aware of the most prevalent and predatory fraud schemes being carried out on online dating sites.

December 27, 2019 7 min read

Opinions expressed by *Entrepreneur* contributors are their own.

The online dating industry is big and profitable. Online dating site Bumble, owned by MagicLabs, is valued at $3 billion and Match Group, which owns sites like Tinder, Hinge, and Match.com, reported $1.7 billion in revenue in 2018. Love is a big business.

But for me, personally, online dating is no laughing matter. Every year, thousands of people are catfished online and it can take a toll – not just financially, but emotionally, too. A "catfish" is defined as someone who creates a false online identity with the intent of defrauding someone, seeking revenge or commit identity theft.

As a public figure, my image and likeness have been used in a

number of dating sites and social media platforms. It might sound like fun and games until someone gets hurt – and that's exactly what happened recently.

A few months back, the BBC reached out to me regarding their show, *For Love or Money*. A woman, Rachel, had been scammed by a man calling himself "Henrick Bjorn" and using my image to communicate with her. He was even able to create a video image that looked like me and spoke with her on Skype numerous times. She was convinced I was the man she fell in love with, which is really infuriating. Since Rachel is in the UK, and the show is filmed there too, the producers Skyped me (the real me) in so I could meet her, reassure her, and offer her consolation and support after this harrowing experience.

Related: How to Growth Hack Online Dating

The tricks and technology these scammers are able to conjure is something straight out of a spy movie! It's disgusting the length that some people will go through to inflict pain.

I've been married to my beautiful wife, Tami, for 37 years and these online scammers have been using my personal pictures, some of which include my grandchildren, to mislead women and even steal their money. My sympathy goes out to everyone who has been scammed because it's more common than we think.

According to the Federal Trade Commission, online dating scams are the highest total reported scam – and that's what *reported*. In 2016 in the U.S., $220 million dollars were stolen by these criminals and in 2018, $143 million dollars were reported lost.

These scammers are the lowest of the low. They not only hijack the photos of well-known celebrities or executives like me, but they often position themselves as having a career or title that keeps them away from their victims. They say they have a job traveling overseas or are in the military. Anything to keep the ruse going and avoid person-to-person contact.

After gaining their victim’s trust, they will position an emergency or some type of need for immediate cash or gift card. The Federal Trade Commission (FTC) has a handy tips sheet on their site and even a video on YouTube that explains the tactics these scoundrels use and how to report it. This is exactly how each scammer has led victims along when they’ve used my image.

So, how as executives in the c-suite, entrepreneurs, and thought leaders, do we protect ourselves and our personal brands from these online trolls? Here are three things you can do immediately if this is happening to you:

Report it

I always report this whenever possible – to as many agencies as I can. Because this happens to me all over the world, this can prove challenging. But make sure you report it to your local police, to the FTC and to the site where your image was used. If you’re on one site then most likely you’re on twenty more, all with different names.

Search the internet

As the busy executives that we are, we don’t have the time to search the internet for all of the images we’ve taken over the years to see how they’ve been used. That is why I have my public relations and social media team frequently check across the internet for my image and other representations of my brand to make sure everything is being used as it was intended.

You can do things like a reverse image search from your phone. I recommend you try it and see what comes up. It’s come to the point where we check online dating sites to see if criminals are using my image to scam others. You have to be a little paranoid to protect yourself. It’s not a bad thing.

I've also had an opportunity to connect directly with many of these victims, women like Rachel from the BBC program, *For Love or Money*. The opportunity for me to share my sympathy with them, to show them I'm a real person and we're both victims here. At least put a human connection there. I know they've lost a lot. Not only money, but they've been hurt.

Protect your personal brand

As I speak to c-suite executives around the world, I coach them on the importance of creating and maintaining their own personal brand. There's a study by Weber Shandwick that proves my point – they estimate that 44 percent of a company's market value can be directly linked to the CEO's reputation. So, I take these attacks on my personal brand seriously as they can have a direct impact on my bottom line.

I also want to make a bold statement – it is incumbent upon the industry to do better. In September, the FTC filed suit against Match Group. One of their claims against Match is that 25-30 percent of the daily sign-ups to their site are scammers. This is unacceptable. It's time for these companies to take what I call a "Hero Mentality" and balance the billions in profit and market cap with "Hero Intensity" and take care of people. I've spoken to that at length in my last book, The Hero Factor. It's time for all companies – big and small, to start taking care of the cogs that make their engines run and that is their people. That's how you elevate your company and your culture. People first, the rest will take care of itself.

Additionally, sites like Facebook, Instagram, Google and dating sites like Match, eHarmony, Tinder and others need to step up and use the best practices, technology, and other methods readily available at their fingertips to ensure their customers and non-customers – the victims here are protected from this harassment and abuse.

This is not a victimless crime. And while no one died, it is still a serious offense and innocent people are getting hurt. It is time companies step up their game and take responsibility, demonstrate true leadership and protect their customers. Anyone using an online dating app or anyone with an online or public-facing profile needs to be aware of one of the most prevalent and predatory fraud schemes out there today. It’s no laughing matter and it’s costing everyone.

https://www.entrepreneur.com/article/344130