Attacco hacker SolarWinds, Italia coinvolta? Riunito il nucleo di sicurezza cibernetica

"L'Italia ha attivato dalle prime fasi della scoperta dell'attacco hacker della piattaforma ***SolarWinds Orion*** *che ha coinvolto i sistemi informatici di enti governativi statunitensi, il* ***Nucleo per la Sicurezza Cibernetica*** *per monitorare un potenziale impatto sulla sicurezza nazionale*".

E' questo l'annuncio dato dall'organismo collegiale italiano a cui è affidato il compito di gestire gli incidenti informatici, guidato dal vicedirettore generale del Dipartimento delle informazioni per la sicurezza (Dis), **Roberto Baldoni**.

Il Nucleo, si legge in una nota del DIS, si è riunito per valutare ogni possibile impatto della campagna di attacchi informatici condotti attraverso la compromissione della piattaforma **SolarWinds Orion** anche sulle reti e sui sistemi nazionali.

L'attacco a SolarWinds: cosa è successo

Lo scorso 13 dicembre i media statunitensi hanno diffuso la notizia del "*più grave attacco informatico da cinque anni a questa parte agli Stati Uniti" che ha coinvolto l'amministrazione Usa.* I cyber attacchi, legati si pensa ai servizi segreti russi con il gruppo APT29 "*Cozy Bear*", hanno

colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale tra cui l'Agenzia per la sicurezza nucleare degli Stati Uniti.

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione. Ma la falla più grave è stata individuata dagli investigatori americaninegli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all'intelligence USA e ai militari.

La backdoor su SolarWinds

Il DIS ricorda che "*il sofisticato attacco introduce una backdoor all'interno della piattaforma SolarWinds attraverso un aggiornamento che permette all'hacker, una volta selezionate le vittime di interesse, di eseguire comandi manuali all'interno dei sistemi della vittima. Ponendo quindi le basi anche per il rilascio di ulteriore codice malevolo volto potenzialmente a spiare o a manomettere ulteriormente i sistemi dell'ente attaccato o dei servizi da esso erogati".*

SolarWinds vanta oltre 300mila clienti, fra cui aziende del calibro di M**icrosoft, Gartner, Mastercard, Mc Donald's, Ing Direct e Volvo**, vendor di sicurezza come **Symantec** e **FireEye**, operatori di telecomunicazione come **Telecom Italia**, **Us Telecom** e **Korea Telecom**.

Sono, inoltre, state avviate tutte le attività di supporto e contatto con i soggetti nazionali preposti a gestire le funzioni ed i servizi essenziali dello Stato (inclusi nel Perimetro di sicurezza nazionale cibernetica), gli operatori di servizi essenziali (previsti dalla Direttiva Europea NIS – Network information System) e gli enti della Pubblica

Amministrazione.

Per il Nucleo di Sicurezza Cibernetica la gravità dell'evento cibernetico e dei suoi effetti resta elevato, per questo il nucleo "*resta in continuo contatto con **"CyCLONe"***, le neo-costituita rete di collegamento europeo, che si propone di agevolare la cooperazione tra le autorità nazionali di cybersecurity in caso di incidenti informatici destabilizzanti.

Il CSIRT

Il Nucleo raccomanda in ogni caso a tutte le organizzazioni che utilizzano la citata piattaforma Orion di **esaminare la problematica con la massima e puntuale attenzione**, avvalendosi a tal fine anche dell'apposita sezione creata sul sito web del CSIRT italiano contenente consigli, aggiornamenti e possibili misure di mitigazione dell'incidente.

https://www.key4biz.it/attacco-hacker-solarwinds-italia-coinvolta-riunito-il-nucleo-di-sicurezza-cibernetica/336708/

Estensioni browser infette da malware, a rischio la sicurezza di milioni di utenti

Il team di ricercatori del *Threat Intelligence* di **Avast** ha

identificato di recente, nascosto in almeno 28 estensioni realizzate da terze parti per i browser **Google Chrome e Microsoft Edge**, un malware con grande capacità di elusione in grado di reindirizzare il traffico di rete verso annunci o siti di phishing e rubare informazioni riservate alle ignare vittime.

Le estensioni e i plug-in dei browser

Per i browser di ultima generazione esiste la possibilità di aggiungere dei componenti che ne consentono la relativa personalizzazione. Si tratta di programmi integrativi che possono essere distinti in plug-in ed add-on. A differenza dei plug-in che sono componenti software che permettono di usufruire di contenuti speciali all'interno delle pagine web visualizzate come filmati, animazioni e presentazioni che il browser non è in grado di gestire, le estensioni sono componenti software che permettono di ampliare le funzionalità, aggiungendo o modificando le caratteristiche dei browser in uso. Si possono trovare estensioni per una miriade di scopi come, ad esempio, aumentare l'accessibilità del browser, gestire download o velocizzare la navigazione e tradurre pagine web.

Gli add-on incriminati

Sebbene sia i plug-in che gli add-on, spesso gratuiti e quasi sempre sviluppati da terze parti, possono essere potenzialmente alterati, senza un adeguato controllo e supervisione, per veicolare software malevolo o propinare servizi illeciti, sono gli add-on per i browser Chrome e Edge le estensioni contaminate oggetto di questa analisi.

Sulla base dei dati raccolti dagli analisti e del numero di download registrati sugli store di Microsoft e di Google

Chrome WEB sarebbero circa tre milioni gli utenti nel mondo ad essere potenzialmente interessati al problema, considerando che queste estensioni malevole sarebbero, per lo più, servizi per note piattaforme social network:

Direct Message for Instagram™, DM for Instagram, Invisible mode for Instagram Direct Message, Downloader for Instagram, Instagram Download Video & Image, App Phone for Instagram, Stories for Instagram, Universal Video Downloader, Video Downloader for FaceBook™, Vimeo™ Video Downloader, Volume Controller, Zoomer for Instagram and FaceBook, VK UnBlock.Works fast, Odnoklassniki UnBlock. Works quickly, Upload photo to Instagram™, Spotify Music Downloader, Upload photo to Instagram™, Pretty Kitty. The Cat Pet, Video Downloader for YouTube, SoundCloud Music Downloader, The New York Times News, Instagram App with Direct Message DM.

Malware e browser: l'attività delle estensioni malevoli

I ricercatori che hanno iniziato a monitorare questa minaccia nel novembre 2020 ritengono che in realtà la campagna possa essere attiva già da diversi anni, grazie all'alta capacità di elusione posseduta dal malware. Dall'analisi dei campioni si è potuto infatti riscontrare che il malware ben nascosto nelle estensioni, resta dormiente per qualche giorno dopo l'installazione e sarebbe anche in grado di rilevare comportamenti di personale esperto nelle attività dell'utente colpito, mantenendo in tal caso la propria inattività.

Il codice dannoso rilevato nelle estensioni basate su javascript consente anche di scaricare ulteriori malware, registrare ed inviare informazioni sui click eseguiti ad un server di comando remoto, effettuare reindirizzamenti URL, geolocalizzare e esfiltrare informazioni sui dispositivi, sistemi operativi e browser usati, consentendo agli attori della minaccia di capitalizzare ogni attività illecita

eseguita.

Come difendersi dai malware

Gli analisti circa l'origine di queste estensioni hanno avanzato diverse ipotesi. Potrebbero essere state create con il malware integrato oppure potrebbero essere state infettate successivamente tramite un aggiornamento nocivo o una iniezione malevola da parte di terzi.

Avast, in ogni caso, ha contattato in modo responsabile i team degli store interessati segnalando l'elenco delle estensioni infette. Anche se Microsoft e Google dopo aver confermato il problema hanno prontamente provveduto a rimuovere gli add-on incriminati, nell'attesa che vengano eventualmente sostituiti resta comunque ancora valida la raccomandazione di disinstallare le estensioni in oggetto, se non ancora fatto, e eseguire quanto prima una bonifica antivirus.

https://www.key4biz.it/estensioni-browser-infette-da-malware-a-rischio-la-sicurezza-di-milioni-di-utenti/336400/

Bitgrail, arrestato l'autore della più grande cybertruffa avvenuta in Italia

Aveva rubato 120 milioni di euro dalla piattaforma informatica "**Bitgrail**", truffando così oltre 230 mila risparmiatori in quello che è stato definitivo il più grande attacco cyber-

finanziario in Italia, uno dei più grandi mai realizzati nel mondo nel settore delle cryptovalute.

La Polizia Postale ha identificato il responsabile: un fiorentino di 34 anni amministratore unico di una società italiana che gestisce una piattaforma di scambio di cryptovalute (exchange), ritenuto responsabile della frode informatica di 120 milioni di euro, di bancarotta fraudolenta e di auto riciclaggio.

La polizia postale italiana pone una pietra miliare a livello mondiale nel settore delle indagini sulle cryptovalute, con un'indagine unica nel suo genere ad alto impatto tecnologico.

Bitgrail: la truffa dei Nano Coin

L'indagine è stata avviata nel febbraio del 2018 dopo la denuncia da parte dell'uomo incriminato del furto di un'ingente somma della cryptovaluta denominata «**NANO**» XRP per un controvalore di circa 120.000.000,00 di euro, realizzato sfruttando un bug del protocollo Nano ed effettuando illecite transazioni, tutte relative a gennaio 2018.

L'indagine ha preso il via nel febbraio del 2018, dopo la denuncia presentata dall'amministratore unico della piattaforma di **exchange**, per il furto di un'ingente somma in criptovaluta "NANO" XRP per un controvalore di circa 120 milioni di euro, realizzato sfruttando un bug del protocollo Nano e compiendo transazioni illecite, tutte relative a gennaio 2018. L'uomo era già noto agli investigatori ai quali forniva Bitcoin per pagare i 'riscatti' delle vittime di criptolocker. Gli inquirenti hanno cominciato a sospettare di lui fin dalle prime battute delle indagini, nonostante collaborasse per non lasciare intendere di essere coinvolto nella vicenda.

La Polizia Postale ed FBI

Le indagini, andate avanti per mesi anche con il supporto dell'FBI, con intercettazioni e complesse attività di analisi informatiche dei database della piattaforma di exchange, hanno portato alla luce le responsabilità dell'uomo e dimostrato che le sottrazioni di criptovaluta sono avvenute in più riprese, a partire da giugno 2017, e che l'uomo consapevolmente non le ha impedite omettendo di implementare la sicurezza della piattaforma con uno dei metodi disponibili resi noti dal Team Nano Developers (Società americana creatrice della criptovaluta), così procurando agli hackers, non ancora individuati, un profitto di circa 11.500.000 XRB, equivalenti a circa 12 milioni di euro, danneggiando più di 230.000 persone in tutto il mondo (peraltro con l'aggravante di aver commesso i fatti con abuso della qualità di operatore del sistema).

https://www.key4biz.it/bitgrail-arrestato-lautore-della-piu-grande-cybertruffa-avvenuta-in-italia/336092/

Attacco hacker al Governo Usa, le falle di SolarWinds colpiscono 275mila clienti

Emergono tanti retroscena nell'attacco hacker dello scorso 12 dicembre che hai coinvolto l'amministrazione USA nel "*più grave attacco informatico da cinque anni a questa parte agli*

Stati Uniti” secondo i media statunitensi.

I cyber attacchi hanno colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale. Dietro a tutto questo, secondo quanto riportato dal **New York Times** e dai media americani c’e la Russia con il gruppo **APT29** “***Cozy Bear***“.

Breccia nei sistemi Microsoft e SolarWinds

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione.

Altra falla individuata dagli investigatori americani è negli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all’intelligence USA e ai militari.

SolarWinds vanta oltre 300mila clienti, fra cui aziende del calibro di M**icrosoft, Gartner, Mastercard, Mc Donald’s, Ing Direct e Volvo**, vendor di sicurezza come **Symantec** e **FireEye**, operatori di telecomunicazione come **Telecom Italia**, **Us Telecom** e **Korea Telecom**. Cuore dell’offerta di SolarWinds è la piattaforma **Orion**, comprensiva di strumenti di gestione, configurazione e analisi delle reti, dei server e delle applicazioni.

Secondo quanto riportata dalla Reuters, l’azienda ha dichiarato che gli upgrade in questione possano esser stati manomessi in effetti tra marzo e giugno 2020 in occasione di un grande attacco informatico, ben pianificato e mirato a degli specifici target.

Il presidente di Microsoft **Brad Smith** ha dichiarato ieri sera

che le informazioni su un coinvolgimento del software di Redmond sono del tutto false: *“Vogliamo rassicurare i nostri clienti che non abbiamo identificato alcuna vulnerabilità nei prodotti o servizi cloud Microsoft nel corso delle indagini”*, aggiungendo successivamente come *“tutti i dati sono al sicuro”.*

La portata dell’azione non è ancora chiara. SolarWinds ritiene che siano stati colpiti tra i 180mila e i 275mila clienti, tra cui tutte le grandi agenzie governative e centinaia di importanti aziende private.

È possibile che siano stati coinvolti anche clienti stranieri di SolarWinds, ma ci vorranno mesi, se non anni, per avere un’idea complessiva di quali siano gli effetti dell’attacco.

https://www.key4biz.it/attacco-hacker-al-governo-usa-le-falle-di-solarwinds-colpiscono-275mila-clienti/335919/

Allarme cybercrime nella Ue ‘Siamo un obiettivo primario’

L’Unione Europea è stata identificata come un **“target primario”** dai cyber criminali globali e per questo deve rinforzare le sue capacità difensive in base al nuovo scenario, secondo la Commissione Ue. A dirlo apertamente è stato ieri il vicepresidente della Commissione Ue **Margaritis Schinas**, in occasione del lancio del nuovo pacchetto di misure Nis 2 che aggiorna la direttiva Nis.

“Ci sono diverse entità, statali e non, che molto

semplicemente vogliono che l'Europa fallisca", ha detto il greco. *"E ci sono molti concorrenti strategici in aree chiave delle nostre politiche e delle nostre industry che utilizzano queste strade per esplorare le nostre vulnerabilità e riuscire a ottenere un vantaggio competitivo. Non c'è dubbio che siamo un obiettivo primario ",* ha aggiunto Schinas.

Un esempio per tutti è il recente cyberattacco del 10 dicembre scorso all'Agenzia Europea del Farmaco di Amsterdam, con l'accesso a informazioni sensibili relative al vaccino per il Covid-19.

"E ci sono molti concorrenti strategici in aree chiave delle nostre politiche e dei nostri settori che utilizzano queste strade per esplorare le nostre vulnerabilità e riuscire a ottenere un vantaggio competitivo. Non c'è dubbio che siamo un obiettivo primario ", ha aggiunto Schinas.

L'alto rappresentante dell'UE **Josep Borrell**, il vicepresidente della Commissione **Margaritis Schinas** e il commissario **Thierry Breton** hanno presentato la strategia ieri in una conferenza stampa a Bruxelles, promettendo che rafforzerebbe la "*resilienza collettiva contro le minacce informatiche*" in tutto il blocco.

Tra le iniziative vi è l'uso di centri operativi per la sicurezza abilitati all'intelligenza artificiale istituiti in tutta l'UE per creare un *"Cyber Shield"* che rilevi i segnali di attacco e possa avviare un'azione preventiva tempestiva.

Un altro è la creazione di una Joint Cyber Unit per garantire una migliore protezione dagli attacchi informatici dannosi e transfrontalieri.

Cos'altro c'è nella strategia?

• Nuove soluzioni europee per rafforzare la sicurezza Internet globale

• Un regolamento per promuovere un Internet of Secure Things
• Una migliore cassetta degli attrezzi diplomatica per prevenire, scoraggiare e rispondere agli attacchi
• Cooperazione rafforzata per la difesa informatica
• Maggiore dialogo sulla sicurezza informatica con i paesi al di fuori dell'UE, insieme a organizzazioni internazionali come la NATO
• La creazione di un'agenda dell'UE per lo sviluppo di capacità informatiche esterne e di un comitato interistituzionale dell'UE per lo sviluppo di capacità informatiche

La strategia da 2 miliardi di euro sarà finanziata dal programma Europa digitale dell'UE e da Orizzonte Europa, con l'aggiunta di investimenti da parte degli Stati membri e dell'industria.
Inoltre, gli esperti prevedono che il numero di dispositivi connessi in tutto il mondo salirà a 25 miliardi entro il 2025. Si prevede che un quarto di questi dispositivi sarà in Europa.

Dichiarazioni di alcuni membri del collegio

Margrethe **Vestager**, Vicepresidente esecutiva per Un'Europa pronta per l'era digitale, ha dichiarato: *"L'Europa è determinata a portare avanti una trasformazione digitale della nostra società ed economia, che dobbiamo quindi sostenere con livelli di investimento senza precedenti. La riuscita della trasformazione digitale, che sta accelerando, si basa sulla fiducia dei cittadini e delle imprese nella sicurezza dei prodotti e dei servizi connessi che utilizzano."*

L'Alto rappresentante Josep **Borrell** ha dichiarato: *"La sicurezza e la stabilità a livello internazionale dipendono più che mai da un ciberspazio globale, aperto, stabile e sicuro in cui siano rispettati lo Stato di diritto, i diritti umani, le libertà e la democrazia. Con la strategia di oggi*

l'UE fa un passo avanti nella protezione dei propri governi, dei cittadini e delle imprese dalle minacce informatiche, esercitando la sua leadership nel ciberspazio, di modo che tutti possano trarre vantaggio dall'uso di Internet e delle tecnologie."

Margaritis **Schinas**, Vicepresidente per la Promozione dello stile di vita europeo, ha affermato: *"La cibersicurezza è un elemento centrale dell'Unione della sicurezza. Non esistono più distinzioni tra minacce online e offline e la dimensione digitale è ormai indissolubilmente connessa alla dimensione reale. L'insieme di misure varate oggi dimostra che l'UE è pronta a usare tutte le risorse e le competenze a sua disposizione per prepararsi e far fronte alle minacce fisiche e informatiche con lo stesso livello di determinazione."*

Thierry **Breton**, Commissario per il Mercato interno, ha dichiarato a sua volta: *"Le minacce informatiche evolvono rapidamente e sono sempre più complesse e adattabili. Per garantire la protezione dei nostri cittadini e delle nostre infrastrutture, dobbiamo giocare d'anticipo: uno scudo europeo per la cibersicurezza resiliente e autonomo consentirà di sfruttare le nostre competenze e conoscenze per reagire più rapidamente, limitare i danni potenziali ed essere più resilienti. Investire nella cibersicurezza significa investire nella nostra autonomia strategica e in un ambiente online sano per il futuro."*

Ylva **Johansson**, Commissaria per gli Affari interni, ha dichiarato: *"I nostri ospedali, i nostri sistemi di trattamento delle acque reflue o le nostre infrastrutture di trasporto sono forti solo quanto gli anelli più deboli della catena: vi è il rischio che le perturbazioni che si verificano in una parte dell'Unione incidano sulla fornitura di servizi essenziali altrove. Per garantire il buon funzionamento del mercato interno e i mezzi di sussistenza di coloro che vivono in Europa, le nostre infrastrutture essenziali devono essere resilienti di fronte a rischi quali catastrofi naturali,*

attentati terroristici, incidenti e pandemie come quella che stiamo vivendo oggi. È proprio questo l'intento della mia proposta sulle infrastrutture critiche."

La nota ufficiale della Commissione UE

Oggi la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza presentano una nuova strategia dell'UE per la cibersicurezza. In quanto componente essenziale della strategia digitale dell'UE Plasmare il futuro digitale dell'Europa, del piano per la ripresa dell'Europa e della strategia dell'UE per l'Unione della sicurezza, la strategia rafforzerà la resilienza collettiva dell'Europa contro le minacce informatiche e contribuirà a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. A prescindere da quali siano i dispositivi connessi, le reti elettriche, i servizi bancari o i trasporti aerei che i cittadini europei utilizzano o le amministrazioni pubbliche o le strutture ospedaliere che frequentano, essi devono potervi accedere con la sicurezza di essere protetti dalle minacce informatiche.

La nuova strategia per la cibersicurezza consente inoltre all'UE di rafforzare la leadership su norme e standard internazionali nel ciberspazio e di intensificare la collaborazione con i partner in tutto il mondo al fine di promuovere un ciberspazio globale, aperto, stabile e sicuro, fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori della democrazia.

La Commissione sta inoltre presentando proposte per affrontare la questione della resilienza sia informatica che fisica dei soggetti critici e delle reti essenziali: una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") e una

nuova direttiva sulla resilienza dei soggetti critici. Questi documenti coprono un'ampia gamma di settori e mirano ad affrontare in maniera coerente e complementare i rischi online e offline attuali e futuri, dagli attacchi informatici alla criminalità o alle catastrofi naturali.

Fiducia e sicurezza al centro del decennio digitale dell'UE

La nuova strategia per la cibersicurezza mira a salvaguardare un'Internet globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza ma anche per proteggere i valori europei e i diritti fondamentali di tutti. Sulla base dei risultati conseguiti negli ultimi mesi e anni, contiene proposte concrete di iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE:

1. **resilienza, sovranità tecnologica e leadership**

In questa linea d'azione la Commissione propone di riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") al fine di aumentare il livello di ciberresilienza dei settori pubblici e privati essenziali: strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali, nonché altre infrastrutture e servizi essenziali che devono rimanere impermeabili in un contesto di minacce sempre più repentine e complesse.

La Commissione propone inoltre di avviare una rete di centri operativi per la sicurezza in tutta l'UE, alimentati dall'intelligenza artificiale (IA), che costituirà per l'UE una vera e propria barriera di cibersicurezza in grado di

rilevare tempestivamente i segnali di un attacco informatico e consentire un'azione proattiva prima che si verifichino danni. Ulteriori misure comprenderanno un sostegno dedicato alle piccole e medie imprese (PMI) nel quadro dei poli dell'innovazione digitale e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i migliori talenti in materia di cibersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza.

2. **Sviluppo della capacità operativa di prevenzione, deterrenza e risposta**

Nell'ambito di un processo progressivo e inclusivo portato avanti con gli Stati membri, la Commissione sta preparando, una nuova unità congiunta per il ciberspazio allo scopo di rafforzare la collaborazione tra gli organismi dell'UE e le autorità degli Stati membri responsabili della prevenzione, della deterrenza e della risposta agli attacchi informatici, comprese le comunità civili, diplomatiche, di contrasto e di difesa informatica. L'alto rappresentante ha presentato proposte per rafforzare il pacchetto di strumenti della diplomazia informatica dell'UE al fine di prevenire, dissuadere e rispondere in modo efficace alle attività informatiche dolose, in particolare quelle che interessano le nostre infrastrutture, le catene di fornitura, le istituzioni e i processi democratici essenziali. L'UE mira inoltre a rafforzare ulteriormente la collaborazione in materia di ciberdifesa e a sviluppare capacità di ciberdifesa all'avanguardia, basandosi sul lavoro svolto dall'Agenzia europea per la difesa e incoraggiando gli Stati membri a sfruttare appieno la cooperazione strutturata permanente e il Fondo europeo per la difesa.

3. **Promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione**

L'UE intensificherà la collaborazione con i partner

internazionali per rafforzare l'ordine mondiale basato su regole, promuovere la sicurezza e la stabilità nel ciberspazio e proteggere i diritti umani e le libertà fondamentali online. Promuoverà norme e standard internazionali che riflettano questi valori fondamentali dell'UE cooperando con i suoi partner internazionali nell'ambito delle Nazioni Unite e in altri contesti pertinenti. L'UE rafforzerà ulteriormente il suo pacchetto di strumenti della diplomazia informatica e intensificherà gli sforzi per la creazione di capacità informatiche nei paesi terzi sviluppando un'apposita agenda esterna dell'UE. Saranno intensificati i dialoghi in materia di cibersicurezza con i paesi terzi e le organizzazioni regionali e internazionali, nonché con la comunità multipartecipativa. L'UE istituirà inoltre una rete per la diplomazia informatica in tutto il mondo per promuovere la propria visione del ciberspazio.

L'UE si è impegnata a sostenere la nuova strategia per la cibersicurezza nei prossimi sette anni con investimenti nella transizione digitale dell'UE a livelli finora mai raggiunti, attraverso il prossimo bilancio a lungo termine dell'UE, in particolare tramite il programma Europa digitale, Orizzonte Europa e il piano per la ripresa dell'Europa. Gli Stati membri sono pertanto incoraggiati a utilizzare appieno il dispositivo per la ripresa e la resilienza dell'UE per rafforzare la cibersicurezza e a fare investimenti a pari livello di quelli dell'UE. L'obiettivo è raggiungere fino a 4,5 miliardi di € di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, in particolare nell'ambito del Centro di competenza sulla cibersicurezza e della rete dei centri di coordinamento e garantire che una parte importante di questi investimenti siano effettivamente attribuiti alle PMI.

La Commissione mira inoltre a rafforzare le capacità industriali e tecnologiche dell'UE in materia di cibersicurezza, anche tramite progetti finanziati congiuntamente dall'UE e dai bilanci nazionali. L'UE ha

l’opportunità unica di mettere in comune le proprie risorse per rafforzare la sua autonomia strategica e promuovere la sua leadership nel campo della cibersicurezza lungo tutta la catena di fornitura digitale (compresi dati e cloud, tecnologie per processori di prossima generazione, connettività ultrasicura e reti 6G), in linea con i suoi valori e le sue priorità.

Ue: Resilienza informatica e fisica delle reti, dei sistemi informativi e dei soggetti critici

È necessario aggiornare le misure esistenti a livello dell’UE volte a proteggere i servizi e le infrastrutture essenziali dai rischi sia informatici che fisici. I rischi per la cibersicurezza continuano a evolvere con la crescente digitalizzazione e interconnessione. Anche i rischi fisici sono diventati più complessi dall’adozione delle norme dell’UE sulle infrastrutture essenziali del 2008, che attualmente riguardano solo i settori dell’energia e dei trasporti. L’obiettivo delle revisioni è aggiornare le norme seguendo la logica della strategia dell’UE per l’Unione della sicurezza, superando la falsa dicotomia tra online e offline e mettendo da parte l’approccio a compartimenti stagni.

Per rispondere alle crescenti minacce dovute alla digitalizzazione e all’interconnessione, **la direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l’Unione (direttiva NIS rivista o “NIS 2”)** proposta riguarderà le entità di medie e grandi dimensioni di diversi settori in base alla loro importanza per l’economia e la società. La direttiva NIS 2 renderà più rigidi i requisiti di sicurezza imposti alle imprese, affronterà la sicurezza delle catene di fornitura e delle relazioni con i fornitori, semplificherà gli obblighi di notifica, introdurrà misure di vigilanza più rigorose per le autorità nazionali e obblighi di

esecuzione più severi e avrà l'obiettivo di armonizzare i regimi sanzionatori in tutti gli Stati membri. La direttiva NIS 2 proposta contribuirà ad aumentare la condivisione delle informazioni e la cooperazione in materia di gestione delle crisi informatiche a livello nazionale e dell'UE.

La **direttiva sulla resilienza dei soggetti critici** proposta estende sia l'ambito di applicazione, sia la profondità della direttiva sulle infrastrutture critiche europee del 2008. Sono ora contemplati dieci settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Nell'ambito della direttiva proposta ciascuno Stato membro adotterebbe una strategia nazionale per garantire la resilienza dei soggetti critici ed effettuerebbe valutazioni periodiche dei rischi. Tali valutazioni contribuirebbero a individuare un sottoinsieme più ristretto di soggetti critici cui incomberebbero obblighi volti a rafforzarne la resilienza di fronte ai rischi non informatici, comprese le valutazioni dei rischi a livello di soggetto, l'adozione di misure tecniche e organizzative e la notifica degli incidenti. A sua volta la Commissione fornirebbe sostegno complementare agli Stati membri e ai soggetti critici, per esempio sviluppando una visione d'insieme a livello dell'UE dei rischi transfrontalieri e intersettoriali e delle migliori pratiche, metodologie e attività di formazione e di esercizio transfrontaliere per testare la resilienza dei soggetti critici.

Garantire la sicurezza delle reti di prossima generazione: 5G e oltre

Nell'ambito della nuova strategia per la cibersicurezza e con il sostegno della Commissione e dell'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, gli Stati membri sono incoraggiati a portare a termine l'attuazione

del pacchetto di strumenti dell'UE per le reti 5G, che definisce un approccio globale e basato sui rischi oggettivi per la sicurezza delle reti 5G e di prossima generazione.

Secondo una relazione pubblicata oggi sull'impatto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G e sui progressi compiuti nell'attuazione del pacchetto di strumenti comune dell'UE comprendente misure di attenuazione, rispetto alla relazione sui progressi compiuti, pubblicata nel luglio 2020, la maggior parte degli Stati membri è già a buon punto nell'attuazione delle misure raccomandate. Ora dovrebbero mirare a completarne l'attuazione entro il secondo trimestre del 2021 e a garantire che i rischi individuati siano adeguatamente mitigati, in modo coordinato, in particolare nell'ottica di ridurre al minimo l'esposizione ed evitare la dipendenza dai fornitori ad alto rischio. La Commissione oggi delinea inoltre gli obiettivi e le azioni chiave volte a portare avanti tale sforzo coordinato a livello dell'UE.

Prossime tappe

La Commissione europea e l'alto rappresentante sono determinati ad attuare la nuova strategia per la cibersicurezza nei prossimi mesi. Entrambi riferiranno periodicamente sui progressi compiuti e informeranno e coinvolgeranno a pieno titolo in tutte le azioni pertinenti il Parlamento europeo, il Consiglio dell'Unione europea e i portatori di interessi.

Spetta ora al Parlamento europeo e al Consiglio esaminare e adottare la proposta di direttiva NIS 2 e la direttiva sulla resilienza dei soggetti critici. Una volta che le proposte saranno concordate e successivamente adottate, gli Stati membri dovranno recepirle entro 18 mesi dall'entrata in vigore.

La Commissione riesaminerà periodicamente la direttiva NIS 2 e

la direttiva sulla resilienza dei soggetti critici e presenterà relazioni in merito al loro funzionamento.

https://www.key4biz.it/allarme-cybercrime-nella-ue-siamo-un-obiettivo-primario/335741/

Leonardo e il furto di dati, perché la cybersecurity non è solamente tecnologia

In questi giorni tra le notizie di cybersecurity più commentate c'è quella relativa al furto di dati del colosso della cyber difesa Leonardo, avvenuto nel corso di due anni (dal 2015 al 2017) ad opera – si legge – di un ex dipendente e un dirigente della società, accusati "*dei delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali e di depistaggio*".

La notizia ha destato non poco scalpore tra gli addetti alla cybersecurity e non solo, considerate anche le possibili ripercussioni per il Paese. Credo però che il punto cruciale non sia quanto avvenuto, pur nella sua gravità. È accaduto e bisogna correre ai ripari, ma ormai non passa giorno senza che ci sia una notizia su attacchi cyber o violazioni di dati. Ci stiamo abituando? Spero di no, perchè questo significherebbe rimanere inerti rispetto ad un futuro che si preannuncia sempre più complicato, e non solo dal punto di vista della sicurezza.

Indipendentemente dunque dal caso in questione e attendendo che le indagini facciano il loro corso, è doveroso fare delle riflessioni su come è stata affrontata fino ad oggi la cybersecurity, un tema che può davvero fare la differenza per qualsiasi Paese. La protezione di informazioni rilevanti e del *know-how* ha sempre rappresentato un obiettivo strategico, ancora di più oggi con la crescente digitalizzazione.

Due anni fa, ad inizio anno 2018 scrissi un articolo su Key4biz auspicando che la cybersecurity non fosse ridotta ad una sorta di farmaco da banco.

Siamo alle soglie del 2021 e i problemi della sicurezza informatica peggiorano, con numeri che crescono anno dopo anno, anche con attacchi altamente sofisticati dal punto di vista tecnico. Non lo dico io, lo raccontano report annuali sulla sicurezza informatica (es. quello italiano pubblicato dal **Clusit** o quello dell'americana **Verizon**) che puntualmente ci allertano sulla situazione catastrofica. Chiaramente, gli approcci risolutivi al 100% non sono fattibili, data la complessità del tema.

Ma è evidente che qualcosa non funziona. Un problema c'è, che però va oltre le colpe di qualcuno. Un problema di approccio e di visione strategica. Si continua a parlare di come le tecnologie sempre più innovative miglioreranno le nostre vite e daranno una svolta alla cybersecurity, ci si incensa quando si raggiunge qualche risultato, spesso effimero rispetto alla

complessa realtà dei fatti.

Dal mio punto di vista ritengo innanzitutto che fino ad oggi sia prevalsa una strategia caratterizzata da una forte chiusura cognitiva (i cosiddetti paraocchi). Vale a dire ci si è concentrati quasi esclusivamente su aspetti puramente tecnologici, quando ormai è opinione sempre più diffusa che la cybersecurity è (soprattutto) un problema che riguarda le persone.

Le soluzioni tecnologiche, per quanto necessarie, arrivano fino ad un certo punto: tutto può essere blindato, ma poi arriva una minaccia interna e tutto crolla. Forse in questi casi un profiler esperto o un criminologo sono più efficaci di un ingegnere informatico! In fin dei conti, tecnologie e dispositivi sono funzionali al raggiungimento degli obiettivi, ma non agiscono da soli. In un modo o nell'altro l'elemento umano è sempre presente. Basti pensare agli attacchi ransomware il cui successo viene il più delle volte determinato dall'apertura di mail di phishing o di allegati per motivi squisitamente umani, dalla curiosità, all'empatia, alla mancanza di consapevolezza, e via dicendo.

È ormai palese che la cybersecurity non è più una questione solo tecnologica; purtroppo, per interessi e posizionamenti vari viene trattata come se lo fosse.

Basta con questa visione fallimentare, ripartiamo dal buon senso! Cominciamo a vederla in un'ottica multidisciplinare, in modo da riuscire a leggere gli scenari digitali in modo più articolato e ricerchiamo le competenze adeguate. Su questo punto, poi, è imperativo fare un ulteriore passo avanti. Le competenze non si improvvisano, un tecnico informatico per quanto bravo non può essere delegato ad occuparsi del tema della consapevolezza digitale, perché questo richiede la conoscenza dei meccanismi umani e sociali relativi ai comportamenti. Non basta andare in aula e dire alle persone di non fare certe cose: ci stupiamo poi perché le persone

continuano a commettere certi errori? Lavorare sul comportamento umano richiede ben altri tipi di competenze.

Parliamoci chiaro, c'è un problema di innovazione. Non tecnologica, ma di visione. Occorre ripartire dalle buone esperienze, svecchiare gli approcci, ridare "nuova linfa" alla cybersecurity, de-contaminandola anche da meccanismi non sempre meritocratici che a lungo andare producono seri danni. Inutile tentare di imitare le buone pratiche degli altri Paesi – correndo loro dietro quasi fosse una corsa ciclistica – se poi schemi e meccanismi proposti rimangono gli stessi.

Si, il cambiamento ci vuole. Ma cominciando dalle persone.

https://www.key4biz.it/leonardo-furto-di-dati-perche-la-cybersecurity-non-e-solamente-tecnologia/334143/

Malware sLoad, in Italia nuova campagna malevola via PEC. L'allarme del CSIRT

È proprio di questa settimana la segnalazione fatta dal **CSIRT** in merito ad una doppia campagna orientata alla distribuzione del malware **sLoad** (noto anche come **StarsLord**), particolarmente insidiosa e che utilizza caselle di posta elettronica certificata (PEC) con un'elevata personalizzazione dei messaggi e l'impiego di allegati con alta capacità di evasione dalle protezioni antivirus.

Il malware Sload

SLoad è il nome di un software malevolo che funziona come downloader/dropper di malware. Le varie ricerche condotte mostrano che i criminal hacker diffondono sLoad tramite campagne malspam, ovvero attraverso gli allegati dannosi ai messaggi di posta elettronica. Questo malware concepito per i sistemi Windows è capace inoltre di raccogliere informazioni di sistema e inviarle a un server di comando e controllo remoto e presidiato (C2), dal quale riceve anche dei comandi. La comunicazione con il suo server C2 avviene, solitamente, per il tramite del servizio BITS che Windows utilizza invece legittimamente per inviare aggiornamenti del sistema operativo.

sLoad appartenendo alla famiglia dei PowerShell downloader è capace in particolare di carpire informazioni riguardo agli elenchi dei processi in esecuzione e alla presenza di client di posta elettronica Microsoft Outlook oltreché acquisire screenshot, analizzare le cache DNS alla ricerca di domini specifici e eseguire il download di altri possibili payload come trojan o ransomware.

L’attacco rilevato in Italia

Secondo il CSIRT, le due campagne massive in corso e tra loro molto simili mirano a diffondere, da caselle PEC verosimilmente compromesse, il malware SLoad tramite un allegato .vbs (“Allegato_XXXXXXXXXXX”) contenuto in archivi compressi con estensione .zip, dove la parte del nome variabile riporta, a seconda delle varianti, un codice numerico o il codice fiscale del destinatario.

Il messaggio e l’oggetto delle

missive PEC

In tutti i casi, i messaggi dei campioni PEC esaminati risultano personalizzati con la ragione sociale ed i riferimenti di determinate aziende italiane (S.r.l. S.n.c) e sollecitano a prendere visione di una fattura insoluta emessa in formato elettronico o addirittura a stamparla su carta per l'efficacia fiscale. Anche l'oggetto è formulato in modo ingannevole. La prima parte variabile che coincide con la ragione sociale dell'azienda è seguita dalla stringa fissa "- Fatture scadute".

La catena d'infezione

Il file di script .vbs, una volta eseguito avvia la catena d'infezione copiando i due eseguibili di sistema powershell.exe e bitsadmin.exe dalle loro directory legittime (rispettivamente c:\Windows\SysWOW64\WindowsPowerShell\v1.0\ e c:\Windows\SysWOW64\) nella directory nascosta %programdata% di Windows, rinominandoli successivamente con un nome casuale in modo da rendere più complessa un'eventuale ricostruzione della catena d'infezione.

Nel dettaglio, spiegano gli analisti del CSIRT, i due file binari copiati e rinominati vengono quindi utilizzati come segue:

- bitsadmin.exe per scaricare il file di secondo stadio e salvarlo nella cartella nascosta %appdata%;
- powershell.exe per eseguire il contenuto del file appena scaricato.

Come difendersi

Non è la prima volta che i criminal hacker diffondono sLoad tramite campagne di spam, inviando e-mail che contengono un allegato malevolo nella speranza che qualcuno lo apra, e molto

probabilmente non sarà nemmeno l'ultima. Nella fattispecie le e-mail PEC includono, come visto, un file di archivio .zip che contiene al suo interno un file di scripting dannoso (.vbs, .vbe, .wsf, .wsc), ma i file che di solito vengono propinati come allegati malevoli possono essere anche documenti .doc, PDF, file eseguibili .exe o JavaScript.

I casi in esame rappresentano dei tentativi di truffa, che dimostrano ancora una volta come il problema, talvolta, non risieda nei sistemi di sicurezza (in questo caso delle PEC) quanto piuttosto nella scarsa gestione e conservazione delle credenziali da parte dei titolari (anch'essi vittime) le cui identità digitali violate vengono, successivamente, utilizzate in modo non autorizzato come mittenti in campagne di questo tipo.

Per tale motivo è altamente consigliato a tutti gli utenti e organizzazioni, per far fronte a questa tipologia di attacchi, di verificare scrupolosamente le e-mail che si ricevono eseguendo anche degli accorgimenti ulteriori di carattere pratico:

- Non aprire allegati o link web presentati in e-mail (anche se PEC) irrilevanti o ricevute da indirizzi sconosciuti e sospetti;
- caricare file e programmi da fonti ufficiali, evitando downloader/installer di terze parti non affidabili;
- scansionare regolarmente i propri sistemi operativi alla ricerca di minacce con antivirus o antispyware affidabili e tenuti aggiornati;
- evitare di abilitare l'esecuzione delle macro nel caso di allegati Microsoft Office apparentemente legittimi;
- fornire periodiche sessioni di formazione finalizzate a riconoscere le possibili e-mail di phishing, alfine di assimilare questi concetti e prendere coscienza che gli atti criminosi possono concretizzarsi anche attraverso gli strumenti informatici.

Malware sLoad, in Italia nuova campagna malevola via PEC. L’allarme del CSIRT

Cybercrime, nel 2021 sempre più attacchi hacker a ospedali e sanità. Il report

Un 2020 senza pace per il settore sanitario. Non solo l’intero settore dovrà lottare contro l’emergenza da covid-19 ma anche contro criminali informatici che, attraverso attacchi hacker alla sanità, non daranno tregua a ospedali, strutture mediche e strutture che si occupano dello sviluppo della distribuzione del vaccino contro il virus.

Lo rivela il nuovo rapporto **Security Predictions 2021,** pubblicato da **FireEye**. Il trend, spiegano gli esperti di sicurezza, non diminuirà nel corso del 2021.

Attacchi hacker sanità: ransomware in aumento

Nel corso del 2020 è aumentato il ricorso a ransomware. Anche in questo caso, spiega il report, gli attacchi sono stati mirati alle strutture mediche nel corso della pandemia. Nel 2021 questo genere di minacce informatiche cresceranno ancora di più e più rapidamente, con un aumento delle tipologie e la frequenza degli attacchi.

In Germania, ricordano gli esperti, un decesso di un paziente è stato generato da un ransomware che, avendo bloccato i computer della struttura, ha obbligato i medici a spostare la persona malata in un altro ospedale e quest'ultima è deceduta durante il trasporto.

Cos'e' il ransomware?

Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

Ci sono due tipi principali di ransomware:

• i cryptor (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);

• i blocker (che bloccano l'accesso al dispositivo infettato).

Come si diffonde?

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

• sembrano apparentemente provenire da **soggetti conosciuti e**

affidabili (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);

• contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

Per approfondire

https://www.key4biz.it/cybercrime-nel-2021-sempre-piu-attacchi-hacker-a-ospedali-e-sanita-il-report/331343/

Bonus Bici, attenzione al sito truffa con la a accentata

Il Bonus Bici è partito oggi con numerose polemiche (oltre 400mila persone in coda), sito in tilt e non funzionante.

Ma un'altra problematica si è insediata all'interno del click day: i siti fake creati apposta dai cybercriminali per sfruttare il traffico intenso per rubare i dati degli utenti o compiere truffe informatiche.

Bonus Bici: tra disservizi e siti fake

Segnaliamo infatti il sito truffa **buonomobilità.it** (con la a accentata), un dominio registrato su **CloudFlare** pur non essendo il sito internet ufficiale.

Il sito con l'accento è un falso e risulta essere molto pericoloso in quanto è stato indicizzato molto bene, perché risultava nei primi posti su Google subito sotto a quello ministeriale.

Il sito corretto a cui accedere è buonomobilita.it.

Bonus mobilità

Il buono mobilità è un contributo pari al 60% della spesa sostenuta – fino a un massimo di 500 euro – per l'acquisto di biciclette, anche a pedalata assistita, veicoli per la mobilità personale a propulsione prevalentemente elettrica (monopattini, hoverboard e segway).

Da oggi è possibile chiedere il bonus attraverso il sito. Sarà un clic-day a causa dei pochi fondi stanziati e "buoni erogati secondo l'ordine temporale di arrivo delle richieste".

https://www.key4biz.it/bonus-bici-attenzione-al-sito-truffa-con-la-a-accentata/328995/

Attacco hacker alla campagna

elettorale di Donald Trump. Rubati 2,3 milioni di dollari in Wisconsin

Un gruppo di hacker ha sottratto al Partito repubblicano nel Wisconsin 2,3 milioni di dollari da un conto corrente dedicato a finanziare attività per la rielezione del presidente Donald Trump.

Lo ha riferito ieri il leader locale dei Repubblicani, **Andrew Hitt,** all'Associated Press.

Il Partito aveva notato attività sospette il 22 ottobre scorso e aveva contattato immediatamente il **Federal Bureau of Investigation (Fbi**), che – spiega Hitt – sta attualmente indagando sull'episodio.

Come è successo

Secondo il presidente del Partito repubblicano nel Wisconsin, gli hacker sarebbero riusciti a manipolare le fatture di quattro fornitori ingaggiati per inviare materiale postale e gadget elettorali per la rielezione di Trump. Così, quando il Partito ha provveduto al saldo dovuto, il denaro è andato agli hacker invece che ai fornitori.

Il Wisconsin è uno degli Stati in bilico che potrebbero avere un ruolo decisivo per l'esito delle elezioni del prossimo 3 novembre. Qui nel 2016 ha vinto Trump con un distacco di meno di 23 mila voti, ma quest'anno i sondaggi danno in netto vantaggio il candidato democratico **Joe Biden**, che sarà proprio nel Wisconsin venerdì prossimo.

Donald Trump e i problemi con la cybersecurity

Il partito repubblicano nelle ultime settimane è letteralmente bersagliato da criminali informatici. L'ultima attacco era stato inflitto martedì al sito della campagna elettorale di Trump *donaldjtrump.com* dove un gruppo di criminal hacker sconosciuti era riuscito a sabotare il sito del Tyconn mandando in onda il seguente messaggio: " *Questo sito è sequestrato. Il mondo ne ha abbastanza delle fake news diffuse quotidianamente dal presidente.*

È ora si conosca la verità", continuava il messaggio aggiungendo che il gruppo di hacker fosse in possesso di informazioni compromettenti sul presidente e la sua famiglia, sia sul coronavirus che sulle prossime elezioni. *"Il trump-gov è coinvolto nell'origine del coronavirus e sta collaborando con gli stranieri per manipolare le elezioni".*

L'attacco informatico, a detta di **Tim Murtaugh**, responsabile della campagna di Trump, non ha avuto conseguenze dal punto di vista di data breach.

https://www.key4biz.it/attacco-hacker-alla-campagna-elettorale-di-donald-trump-rubati-23-milioni-di-dollari-in-wisconsin/328537/