Covid-19: le frodi online si portano via metà dei sussidi USA, grazie al furto dei dati personali

Una notizia che sembra quasi incredibile, quella del **furto dei sussidi di disoccupazione negli Stati Uniti**, sia per la portata del danno economico, sia per il modo in cui le azioni criminali sono state portate a termine, tramite le classiche frodi online.

Si è spesso parlato di quanto sia importante fare attenzione a quello che si fa in rete, come si scelgono le password e come si utilizzano, quali siti web è meglio navigare e che tipo di email è bene aprire e quali no. Quello che è accaduto negli Stati Uniti è **il tipico esempio dell'impatto dei cyber crimine sull'economia di un Paese e sulla vita quotidiana dei suoi abitanti**.

Il cyber crimine si porta via 400 miliardi di sussidi Covid USA in un anno. La pista cinese e russa

Secondo il sito *axios.com*, tramite frodi online di varia natura **gruppi criminali con base in più di un Paese straniero sono riusciti ad entrare in possesso dei fondi pubblici per i sussidi di disoccupazione** per far fronte all'emergenza sociale e sanitaria decretata all'indomani della pandemia di Covid-19.

L'amministratore delegato del sito *id.me*, **Blake Hall**, società

che offre servizi di tutela e difesa delle identità digitali in rete, ha dichiarato: "***A causa delle frodi online gli Stati Uniti hanno perso più di 400 miliardi di dollari durante il 2020,*** *potrebbe esser stato rubato il 50% circa dei sussidi di disoccupazione*".

Haywood Talcove, amministratore delegato di LexisNexis Risk Solutions, ha inoltre aggiunto: "*Il 70% dei soldi rubati ormai avrà già lasciato il Paese, molto probabilmente sarà nelle mani di* ***gruppi criminali in Cina, Russia, Nigeria*** *e altri Paesi. Sono sicuro che questi criminali sono sponsorizzati da enti governativi*".

Un 30% circa, invece, potrebbe esser finito nelle tasche delle bande criminali americane.

I dati personali fondamentali per le frodi online

Come è stato possibile portare a termine diverse operazioni di cybercrime di questo livello a danno dei contribuenti americani, durante un anno così terribile per gli Stati Uniti a causa della pandemia di Covid? Semplice, i truffatori hanno prima fatto **incetta di dati personali in rete, di informazioni sensibili** relative ad ignari cittadini, per poi sfruttarle proprio per richiedere i sussidi al posto loro.

Molti di questi soldi venivano poi di fatto sottratti agli aventi diritto tramite carte di credito e di debito, direttamente allo sportello bancomat, per poi cambiarli in **bitcoin** e trasferire il tutto all'estero.

La cosa grave è che, secondo i siti specializzati in cybersecurity, **tale tipo di frode è oggi offerta nel dark web come servizio on demand, tramite modello "*Software-as-a-Service*"**, allo stesso modo dei ransomware.

Raddoppiati i reclami alla FTC

I reclami alla Federal Trade Commission (FTC) in merito a frodi legate all'identità sono più che raddoppiati nel 2020.

A conferma di quanto stiamo scrivendo, a metà del 2020, l'ispettore generale del Dipartimento del lavoro degli Stati Uniti ha dichiarato al Congresso che le indennità di disoccupazione rubate potevano raggiungere i 26 miliardi di dollari.

Un dato eclatante, ma ancora non si sapeva che nella sola California tali pratiche fraudolente online avevano già sottratto allo Stato e ai cittadini 11 miliardi di dollari.

Il Repubblicano **Kevin Brady**, membro della Camera dei Rappresentanti per lo stato del Texas, aveva ipotizzato lo scorso marzo che il volume totale delle frodi poteva superare i 63 miliardi di dollari, stando ad un articolo dell'Associated Press. Purtroppo si sbagliava e anche di grosso, perché ora si ipotizza che la somma totale sia quasi sette volte maggiore.

https://www.key4biz.it/covid-19-le-frodi-online-si-portano-via-meta-dei-sussidi-usa-grazie-al-furto-dei-dati-personali/364044/

L'Agenzia per la cybersecurity, il via libera

dal Governo

Il consiglio dei ministri ha dato il via libera al decreto-legge che istituisce l'Agenzia per la Cybersicurezza Nazionale (**ACN**), la sua presidenza e definisce l'architettura nazionale di Cybersicurezza. Tra i motivi che hanno determinato queste scelte, è scritto nel decreto, "…*la cybersicurezza è posta nel PNRR a fondamento della trasformazione digitale*".

Agenzia per la cybersicurezza Nazionale, tutti i dettagli

Il provvedimento completa la strategia di cyber-resilienza nazionale, avviata con la disciplina sul perimetro cibernetico, e accresce, attraverso la promozione della cultura della sicurezza cibernetica, la consapevolezza del settore pubblico, privato e della società civile sui rischi e le minacce cyber.

L'Agenzia opererà sotto la responsabilità del Presidente del Consiglio dei ministri e dell'Autorità delegata per la sicurezza della Repubblica e in stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica e sarà tra l'altro incaricata di:

- esercitare le funzioni di Autorità nazionale in materia di cybersecurity, a tutela degli interessi nazionali e della resilienza dei servizi e delle funzioni essenziali dello Stato da minacce cibernetiche;
- sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione, per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security

Incident Response Team (CSIRT) italiano e l’avvio operativo del Centro di valutazione e certificazione nazionale;

- contribuire all’innalzamento della sicurezza dei sistemi di Information and communications technology (ICT) dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, delle pubbliche amministrazioni, degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD);
- supportare lo sviluppo di competenze industriali, tecnologiche e scientifiche, promuovendo progetti per l’innovazione e lo sviluppo e mirando a stimolare nel contempo la crescita di una solida forza di lavoro nazionale nel campo della cybersecurity in un’ottica di autonomia strategica nazionale nel settore;
- assumere le funzioni di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza e attività ispettive negli ambiti del perimetro di sicurezza nazionale cibernetica, della sicurezza delle reti e dei sistemi informativi (direttiva NIS), e della sicurezza delle reti di comunicazione elettronica.

Inoltre, il decreto istituisce il Comitato interministeriale per la cybersicurezza (CIC) e prevede specifici poteri di controllo da parte del Comitato parlamentare per la sicurezza della Repubblica (COPASIR).

Infine, quale tempestivo adeguamento alla normativa europea, il Governo ha individuato l’Agenzia quale Centro nazionale di coordinamento italiano, che si interfaccerà con il “Centro europeo di competenza per la cybersicurezza nell’ambito industriale, tecnologico e della ricerca” di recente istituzione, concorrendo ad aumentare l’autonomia strategica europea nel settore.

Alle 8:45 di questa mattina **Franco Gabrielli** ha illustrato al **COPASIR** il decreto legge, atteso in Consiglio dei ministri,

che andrà ad istituire l'Agenzia per la Cybersecurity Nazionale (**ACN**), l'Agenzia nazionale pubblica che avrà il compito di gestire la sicurezza cibernetica del Paese, ridisegnando l'architettura della difesa italiana dalle minacce cyber.

Il COPASIR è chiamato ad esprimere un parere sul testo prima dell'approvazione da parte del Governo e poi la conversione in legge da parte del Parlamento. Il Paese, per Gabrielli, ha una fragilità *"per mancanza dei consapevolezza dei rischi, per un deficit di cultura su questi temi: purtroppo siamo molto in ritardo e dobbiamo camminare a passi molto svelti".*

L'Agenzia per la Cybersecurity Nazionale, le caratteristiche

È un'Agenzia ad hoc per la cybersecurity. Un'agenzia pubblica, dove l'attività di stretta intelligence resterà comunque in capo al Dipartimento delle informazioni per la sicurezza (Dis). Prima di volare in Cornovaglia per il G7, il premier **Mario Draghi** ha voluto accelerare su uno dei punti chiave dell'Alleanza Atlantica che, da qui ai prossimi giorni, potrebbe essere rinsaldata tra l'Italia e l'amministrazione **Joe Biden** e adattata l'iniziativa NATO 2030 e la cooperazione fra la NATO e l'Unione Europe.. Il decreto per l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (Acn) è quasi pronto ed è stato oggetto, ieri, di una cabina di regia a Palazzo Chigi alla quale – ad eccezione di **Giancarlo Giorgetti**, assente per motivi di agenda – hanno partecipato i capidelegazione della maggioranza e il sottosegretario ai Servizi Franco Gabrielli.

L'Agenzia per la Cybersecurity

Nazionale, come funzionerà? 300 dipendenti, entro il 2027 potrebbe arrivare a 800

L’Agenzia sarà istituita in capo alla presidenza del Consiglio, i suoi vertici saranno di nomina governativa. L’agenzia dovrà avere anche un ruolo di governance. Intervenire, per esempio, se non prevenire, quando si intravedono rischi sull’appalto di un comune per lo sviluppo di una smart city. Fronte, quest’ultimo, dove sono già noti gli alert dell’intelligence, compresi gli americani, sugli investimenti – e relative minacce – cinesi. Nasce il Cisc (comitato internazionale per la sicurezza cibernetica) in analogia al Cisr (sicurezza intelligence), si aggiungono i ministri dell’Innovazione tecnologica dell’Università.

La dotazione iniziale sarà di 300 dipendenti, entro il 2027 potrebbe arrivare a 800. Nella concezione della nuova architettura cibernetica, inoltre, c’è un profilo strategico mirato: il rilancio e lo sviluppo delle imprese italiane. Non soltanto nella protezione dagli attacchi. Ma anche nella capacità di sviluppare start up e aziende di un settore in crescita continua. Oggi diversi software necessari per la sicurezza cibernetica sono importati dall’estero, con tutte le implicazioni immaginabili. Il decollo di quelli italiani è il sottotitolo della nuova politica cyber di palazzo Chigi.

Il direttore dell’Agenzia

L’Agenzia avrà un direttore (sarà un dirigente di prima fascia dell’amministrazione dello Stato) con un mandato di quattro anni (sarà rinnovabile). Sarà posta sotto il controllo del Copasir. Il decreto contiene 20 articoli, l’Agenzia sarà pubblica, i contratti saranno equiparati a quelli della Banca d’Italia. Ai 300 di partenza si aggiungerà personale assunto a tempo determinato. Sotto il vertice ci saranno sei direzioni.

All’interno sarà contenuto anche il Nucleo per la sicurezza cibernetica, che attualmente si trova nel perimetro del Dis. L’agenzia lavorerà sotto la presidenza del Consiglio dei ministri e l’Autorità delegata, in raccordo con il nuovo Comitato interministriale per la sicurezza cibernetica.

Agenzia per la Cybersecurity Nazionale, l’obiettivo

L’obiettivo dell’Agenzia per la Cybersecurity Nazionale è rendere il sistema informatico italiano impermeabile a qualsiasi attacco. Ma eventuali azioni di contro-hackeraggio restano appannaggio dell’intelligence italiana. Alla vigilia dell’arrivo di Biden in Europa, il governo italiano vuole portare in dote al presidente degli Stati Uniti l’Agenzia per la Cybersecurity Nazionale. Se l’Italia sarà più resiliente agli attacchi informatici i benefici non saranno solo per il nostro Paese, ma per tutta la Rete.

Biden: “In virtù dell’art. 5 del Patto atlantico, alleati anche contro attacchi informatici alle nostre infrastrutture critiche”

Infatti, Biden sul *Washington Post* ha espresso la volontà di estendere l’articolo 5 dell’Alleanza atlantica, ossia il dovere di mutua difesa, agli attacchi informatici. *“A Bruxelles, al vertice della NATO, affermerò”,* ha scritto Biden*, “l’impegno incrollabile degli Stati Uniti nei confronti dell’articolo 5 e per garantire che la nostra alleanza sia forte di fronte a ogni sfida, comprese le minacce come gli attacchi informatici alle nostre infrastrutture critiche”.*

Cybersecurity. Prima dimenticata da Biden nel suo piano, ora in cima all'agenda della Nato

Dopo l'attacco informatico che ha bloccato l'oleodotto Colonial Pipeline, il presidente Usa ha posto la Cybersecurity, dimenticata nel suo piano da 2 trilioni di dollari *"American Jobs Plan*, in cima alla sua agenda e il Dipartimento di Giustizia Usa sta elevando le indagini sugli attacchi ransomware, scrive la *Reuters*, a una priorità simile a quella del terrorismo.

https://www.key4biz.it/lagenzia-per-la-cybersecurity-alle-ore-17-il-via-libera-dal-governo-scarica-lultima-bozza-del-decreto/363956/

RockYou2021, pubblicata in rete collezione di 8 miliardi di password rubate

Ogni occasione è buona per ricordare a tutti di **prestare più attenzione alla creazione delle password e al loro utilizzo**. La superficialità con cui si tratta l'argomento è sbalorditiva, soprattutto leggendo le notizie di cybersecurity che regolarmente sono pubblicate in rete sull'argomento. Tra cui il **mega data leak** appena scoperto e denominato "***RockYou2021***".

Secondo quanto riportato dai media e dai siti specializzati, si tratta di **un bottino online di 8,4 miliardi di password rubate**, 100 GB di file in formato *.Txt*. Sicuramente una collezione impressionante di leak e breach di password avvenuti negli ultimi anni.

La raccolta è stata pubblicata su un popolare hacking forum internazionale e stando all'autore del post contiene password con carattere "*Non ASCII*" (da 6 a 20 caratteri).

Il nome "*RockYou2021*" dovrebbe rimandare ad una precedente ed altrettanto storica razzia di password avvenuta nel 2009 (in quel caso furono sottratte 32 milioni di password), al tempo denominata "*RockYou*".

Considerando le dimensioni del bottino, il consiglio è verificare sue la propria password sia ancora sicura, magari con il servizio "*Web Have I Been Pwned*", oppure se si è stati vittima di violazione di dati personali.

I consigli degli esperti sono sempre gli stessi: cambiare password se si è nel dubbio; creare password più complesse (non importa se sono difficili da ricordare); abilitare l'autenticazione a due fattori (2FA); esaminare sempre con attenzione le email che si ricevono, ma anche le telefonate e i messaggi in chat; non scaricare o eseguire file ambigui, non attesi o che arrivano da mittenti sconosciuti.

https://www.key4biz.it/rockyou2021-pubblicata-in-rete-collezione-di-8-miliardi-di-password-rubate/363936/

Ransomware: la JBS USA ha pagato il riscatto, 11 milioni di dollari in bitcoin. FBI teme aumento attacchi

Ransom pagato, JBS ha preferito negoziare con i criminali

Alla fine anche la **JBS**, gigante brasiliano dell'industria della carne a livello globale, ha pagato il riscatto ai cyber criminali che nei giorni scorsi avevano portato un duro **attacco ransomware** ai suoi impianti, rallentando o rendendo impossibile le attività industriali.

Secondo quanto appreso dal *Wall Street Journal*, il pagamento è stato di **11 milioni di dollari, tutti in bitcoin**. Una scelta difficile, ha spiegato nell'articolo l'amministratore delegato di JBS America, **Andre Nogueira**, ma necessaria per limitare ogni potenziale nuovo attacco all'intera rete di distribuzione dei prodotti, con ricadute enormi sull'intero indotto, compresi i clienti finali: ristoranti, negozi di alimentari, grande distribuzione, gli agricoltori e di nuovo gli allevatori.

"*Il pagamento del riscatto è avvenuto dopo che quasi tutti gli impianti erano stati riavviati*", ha affermato Nogueira. La JBS negli Stati Uniti è la più grande impresa di trasformazione

della carne in prodotti alimentari, soprattutto carni bovine, suine e avicole.

Dietro l'attacco il gruppo REvil, con base in russia

Al pagamento non sembra si sia opposta l'**FBI**, il Federal Bureau of Investigation, anche se l'agenzia federale è ufficialmente contraria ad ogni tipo di negoziazione con i cyber criminali. Alti funzionari della Casa Bianca hanno commentato il fatto, riconoscendo la difficoltà di prendere ogni tipo di decisione quando si è sotto attacco, soprattutto per l'impatto economico ed industriale che ne deriva.

L'FBI ritiene che il gruppo di cyber criminali molto probabilmente ha operato da territorio russo, attribuendo l'attacco al **gruppo REvil**, una tra le tante bande del ransomware operative in rete. Ad oggi, ha commentato l'ad di JBS America, non è ancora chiaro come abbiano fatto i cracker a bucare le difese della società.

I dati dei clienti, dei fornitori e dei dipendenti non sono mai stati in pericolo, ha precisato Nogueira, perché i database sono al sicuro e protetti da sistema di crittografia avanzato. Inoltre tutti i dati sono backuppati in seconde linee: "*è grazie a questo sistema che siamo stati in grado di far ripartire gli impianti*", ha aggiunto il manager.

FBI contraria ai pagamenti, anche il Dipartimento dell'Energia chiede una legge che li vieti

Anche l'altro grande caso di attacco ransomware negli Stati Uniti, alla **Colonial Pipeline**, si è risolto con un pagamento in bitcoin agli aggressori. Anche qui si è preferito

contrattare con i criminali del web per evitare ulteriori danni, o peggiori conseguenze agli oleodotti e all'approvvigionamento di carburanti per i tanti Stati raggiunti dal servizio di rifornimento.

A pagamento avvenuto, però, l'FBI è poi intervenuta recuperando 2,3 milioni di dollari su 4,4 milioni totali.

Il segretario all'Energia degli Stati Uniti, **Jennifer Granholm**, ha comunque ribadito il no convinto ad ogni trattativa con questi criminali e soprattutto ha chiesto un confronto più ampio sulla possibilità di vietare il pagamento del riscatto, invitando il Congresso ad affrontare il problema.

Dello stesso parere anche l'FBI, secondo cui pagare riscatti è il miglior modo per sostenere l'industria del crimine online, che è in fortissima espansione e che preoccupa sempre di più, peraltro senza alcuna certezza di tornare in possesso di record di dati o sistemi presi in ostaggio.

https://www.key4biz.it/ransomware-la-jbs-usa-ha-pagato-il-riscatto-11-milioni-di-dollari-in-bitcoin-fbi-teme-aumento-attacchi/363914/

Adolfo Urso nuovo presidente del Copasir. Meloni: "Agirà per l'interesse dell'Italia"

Adolfo Urso, senatore di **Fratelli d'Italia**, è stato eletto

presidente del **Copasir** con 7 voti a favore. Una scheda bianca. Assenti, i due leghisti Raffaele Volpi (l'ex presidente) e Paolo Arrigoni.

Urso ha incassato i voti di M5S, che ha tre membri a San Macuto, Dieni, Castiello e Cattoi, di Fi con Fazzone e Vito, del Pd (Borghi) di Iv (Magorno). Sette voti in totale, che sono uno in più di quanto basta (servivano sei preferenze) per l'investitura alla guida del Comitato di controllo dei servizi italiani, ruolo chiave e di snodo delle più delicate vicende che riguardano la sicurezza del Paese.

Così, dopo mesi di stand-by, ora con il nuovo presidente il **Comitato per la Sicurezza della Repubblica** torna a svolgere la sua attività in un momento così sensibile per la sicurezza nazionale, quanto mai esposta alle minacce cibernetiche.

Dieni (M5S) e segretario COPASIR: *"Buon lavoro a Urso ed ora serenità tra i membri per svolgere al meglio le attività"*

*"Il **Movimento 5 Stelle ha contribuito a sbloccare** l'impasse cui era arrivato il COPASIR, votando favorevolmente il Senatore di Fratelli d'Italia – Adolfo Urso – come Presidente del Comitato nel rispetto della legge 124/2007. **Ad Urso vanno i miei più sinceri auguri di buon lavoro**. C'è molto da fare e quello che auspichiamo è che si possa ritrovare la totale serenità per svolgere al meglio tutte le attività previste" –* ha dichiarato **Federica Dieni (M5S) – Segretario del COPASIR**.

https://www.key4biz.it/adolfo-urso-il-nuovo-presidente-del-copasir-che-torna-a-svolgere-la-sua-attivita/363844/

Sicurezza informatica, industria automobilistica in ritardo di 10 anni. Ecco le nuove minacce

Un Report sulle nuove minacce alla sicurezza dei mezzi

Le auto connesse in rete sono ormai una realtà ed in futuro aumenterà fortemente il loro numero sulle nostre strade. Di pari passo, però, cresce anche il livello ed il numero di minacce informatiche a questo tipo di veicoli che caratterizzano la nuova mobilità.

Secondo uno **studio** pubblicato dal CyLab della Carnegie Mellon University e presentato all'IEEE Symposium on Security & Privacy sono già state individuate delle **nuove vulnerabilità informatiche per i veicoli connessi in rete** o *connected vechicles* sul mercato.

Un ritardo di dieci anni nella cybersecurity dei veicoli connessi

in rete

“*Se sfruttate bene, queste vulnerabilità consentono ai cyber criminali di superare i sistemi IDS i un veicolo connesso in rete e condizionare il funzionamento di vari componenti chiave, tra cui il motore, che da remoto può essere benissimo spento*”, ha spiegato **Sekar Kulandaivel**, Ph.D. di CyLab e principale autore dello studio.

“*Fondamentale per contrastare efficacemente questo tipo di cyber attacchi è quindi sviluppare una nuova classe di sistemi IDS nei veicoli di nuova generazione, a cui affiancare un aggiornamento dei livelli di sicurezza degli hardware*”, ha aggiunto Kulandaivel.

“*La cybersecurity non è stata ancora presa in considerazione come si deve da parte dell’industria automotive* – ha affermato l’autore del Report – *che di fatto è rimasta indietro di almeno dieci anni rispetto ai livelli di sicurezza informatica dei personal computer*”.

La sicurezza dei sistemi di controllo IDS

Ggli **IDS** o *Intrusion Detection Systems* sono sistemi software e hardware (a volte una combinazione dei due) dedicati all’identificazione di accessi non autorizzati a dispositivi e reti locali, come quelli messi in atto da cracker e cyber criminali in tutto il mondo.

A differenza del *firewall,* che con una lista di controllo degli accessi definisce un insieme di regole che i pacchetti di informazioni devono rispettare per entrare o per uscire dalla rete locale, un IDS controlla solo lo stato di tali pacchetti, che girano all’interno della rete locale, confrontandolo con situazioni pericolose già successe prima o con situazioni di anomalia definita dall’amministratore di

sistema, subendo però eventuali intrusioni/violazioni dovute a nuova minacce non conosciute.

Lo studio ha dimostrato, inoltre, attraverso diversi test su auto già in commercio, che una determinata componente del veicolo presa di mira da un cyber attacco potrebbe avere più di un impatto negativo anche sulle altre, tipo effetto domino, spesso senza essere individuato in tempo.

Deve essere cyber anche l'energia

Tra i target del cyber crimine ci sono anche le strategie messe in pratica dalle case automobilistiche per migliorare le performance energetiche. Alla riduzione dei consumi di ogni singola funziona o componente è preposta l'Unità di controllo elettronico o **Ecu** (*Electronic control unit*).

L'ecu è un sistema di controllo software embeddato nella componente specifica, che attraverso appositi sistemi o *gate* permette di spegnere tutto ciò che non è necessario sul momento, così da risparmiare energia. Secondo i ricercatori, un attacco informatico da remoto potrebbe tranquillamente impedire l'attivazione di questo sistema, rendendo impossibile il consumo di energia e quindi, ad esempio nelle auto elettriche, abbattendo anche di molto l'autonomia e l'efficienza, ma anche la sicurezza del veicolo nel suo complesso.

Secondo un recente sondaggio HSB, **il 35% degli automobilisti americani teme che un virus informatico sia in grado di provocare un incidente**, o possa rubare i dati personali e più sensibili, o inserire un software infetto per il controllo dei sistemi operativi del veicolo.

https://www.key4biz.it/sicurezza-informatica-industria-automobilistica-in-ritardo-di-10-anni/363836/

Nasce l’Agenzia per la cybersicurezza nazionale, oggi cabina di regia con Draghi

Si chiamerà Agenzia per la Cybersecurity Nazionale (**ACN**), il nome è stato svelato da *Repubblica*, l’Agenzia nazionale pubblica che avrà il compito di gestire la sicurezza cibernetica del Paese. Oggi pomeriggio si è svolta a Palazzo Chigi una riunione della cabina di regia, presieduta dal premier Mario Draghi, sull’Agenzia per la cybersecurity e venerdì sarà varato dal Consiglio dei ministri il decreto-legge che la istituisce e definisce la governance della cybersecurity in Italia.

Si concretizza il progetto di Gabrielli: *“Dar vita a un’Agenzia ad hoc per gestire in modo olistico la sicurezza cibernetica, che non può essere più affidata al Dis che deve occuparsi di Intelligence*“

Dunque sta per concretizzarsi l’idea di **Franco Gabrielli**, Sottosegretario alla Presidenza del Consiglio con delega agli 007, che annunciò la creazione dell’agenzia per la

cybersecurity in questa videointervista esclusiva di Cybersecurity Italia.

[embedded content]
“*È il momento di dar vita a un’Agenzia ad hoc per gestire in modo olistico la sicurezza cibernetica, che non può essere più affidata al Dis che deve occuparsi di Intelligence*”, ci disse Gabrielli.

Agenzia per la cybersicurezza nazionale, a cosa serve?

Così il Dis, guidato da **Elisabetta Belloni**, può svolgere a tempo pieno la sua missione principale: coordinare le due agenzie di intelligence, **Aise** e **Aisi**, mentre l’Agenzia per la Cybersecurity Nazionale sarà il referente unico per l’Unione Europea e per le aziende e i centri di ricerca italiani specializzati nella sicurezza cibernetica.

https://www.key4biz.it/nasce-lagenzia-per-la-cybersicurezza-nazionale-e-nuova-governance-della-cybersecurity-in-italia/363800/

Internet non funziona: down numerosi siti di aziende, giornali e Governi di tutto il mondo

Giù i siti web di giornali e testate nazionali, di Governi ed organizzazioni internazionali per un probabile disservizio a catena su scala planetaria. Le prime frammentarie notizie sono state pubblicate sulle pagine ancora in piedi di altre fonti di informazione, come la *Reuters*.

The Guardian, il *Financial Times*, *Bloomberg News*, la CNN, il sito del Governo della Gran Bretagna, il *New York Times*, solo per citare alcuni grandi nomi, al momento (attorno alle 12:00) sono tutti offline, non raggiungibili in rete.

Molte anche le aziende, tra cui le Big Tech, che risultano coinvolte in questo **blackout di internet** tutt'ora in corso: Amazon, Reddit, Twitch, PayPal, Spotify.
La **lista dei siti down** proposta da *downdetector.it* è lunga.

Al centro di questo enorme disservizio di rete ci potrebbe essere **Fastly**, global provider di servizi cloud, con sede in San Francisco, su cui si appoggiano molti siti web di tutto il mondo.

Difficile dire se si sia trattato di cyber attacco o di incidente informatico interno al cloud provider. Al momento, dopo un primo allarme generale, sembrerebbe che alla base del grande down di internet ci sia un malfunzionamento.

Fastly ha reso noto di aver avviato tutte la operazioni di ripristino necessarie, comprese le indagini internet per capire cosa sia accaduto ai suoi sistemi.

Al di fuori delle cause alla radice del grave blackout di internet avvenuto stamattina e in parte in via di risoluzione, secondo bloomberg.com, rimane un'evidenza chiara: in tempi di rapida convergenza ed interdipendenza tra reti e risorse, servizi e contenuti, è lampante l'**urgenza di una maggiore**

autonomia tecnologica di ogni singola organizzazione dal contesto, proprio per non finire schiacciati dall'effetto domino di qualsiasi tipo di incidente di questa portata.

https://www.key4biz.it/internet-non-funziona-down-numerosi-siti-di-aziende-giornali-e-governi-di-tutto-il-mondo/363707/

Cyber attacco alla JBS, è un ransomware. L'industria della carne USA si ferma, aumentano i prezzi

Nella notte tra il 31 maggio e il 1° giugno è stato annunciato un **attacco informatico alla multinazionale dell'agroalimentare JBS**, con ripercussioni gravi sui server in Nord America e Australia. In quest'ultimo Paese è stato predisposto il blocco delle attività produttive negli impianti e i dipendenti sono stati invitati a rimanere a casa.

JBS, specializzata in prodotti di manzo, pollo e maiale, è una delle più grandi aziende alimentari al mondo. Oltre che in Brasile e negli altri Paesi dell'America Latina, è presente in Stati Uniti, Canada, Australia, Nuova Zelanda e Regno Unito, con grandi esportazioni verso la Cina e l'Asia in generale.

JBS: è stato un ransomware e l'attacco potrebbe provenire dalla Russia secondo Washington

Il Governo americano ha dichiarato ieri che l'attacco informatico è stato portato con tecnica **ransomware** e che **l'organizzazione criminale potrebbe avere base in Russia**, secondo quanto riportato in un articolo pubblicato dalla *Reuters*.

Gran parte delle attività produttive dovrebbero riprendere oggi, visto che secondo la JBS gran parte dell'attacco informatico è stato contrastato e contenuto.

Gli impianti di macellazione della carne e della lavorazione industriale di prodotti alimentari destinati alle catene dei supermercati sono stati fermati anche negli Stati Uniti, a seguito dell'attacco.

Secondo le stime del Dipartimento dell'Agricoltura del Governo degli Stati Uniti, sempre **a causa dell'attacco ransomware alla JBS, i produttori di carne statunitensi hanno macellato il 22% in meno di bestiame**, rispetto a una settimana fa, e **il 18% in meno rispetto allo stesso periodo del 2020**. Anche la lavorazione del maiale è fortemente diminuita in questi giorni.

Una situazione di crisi che potrebbe portare ad un **aumento dei prezzi dei prodotti a base di carne** e della stessa carne lavorata e venduta dalla JBS e dall'interno indotto collegato alla corporation. Al momento si stima un aumento dei prezzi **tra l'1 e il 2% in più**.

Domande ancora aperte: a quanto

ammonta il riscatto? Quali dati sensibili sono stati raggiunti?

Rimane il dubbio su chi ci sia davvero dietro l'attacco informatico. La Casa Bianca ha puntato il dito contro un'organizzazione ancora senza nome che opera dai territori russi, ma non si sa molto altro. C'è inoltre ancora aperta la questione danni: quanti e quali sono i danni economici e all'infrastruttura di rete IT della multinazionale? Quali i danni invece alla rete di distribuzione dei prodotti alimentari derivati dalla macellazione della carne negli Usa, in Canada, in Brasile e in Australia?

Un attacco ransomware si basa su un concetto semplice: arrivare ai dati sensibili e "sequestrarli" per poi richiedere il riscatto per la loro liberazione. Che tipo di dati sensibili della JBS sono stati raggiunti dai cyber criminali? Quanto ammonta il riscatto? Che ripercussioni avrà sul mercato della carne americano e anche cinese?

https://www.key4biz.it/cyber-attacco-alla-jbs-e-un-ransomware-lindustria-della-carne-usa-si-ferma-aumentano-i-prezzi/363191/

Governo USA lancia nuova tecnologia "Shadow figment": una guerra dei cloni contro i cyber criminali

L’emergenza sanitaria legata alla pandemia di Covid-19 ha rappresentato una grande occasione per i gruppi cyber criminali. **A livello mondiale, nel 2020, sono stati registrati 1.871 attacchi informatici di livello ritenuto “grave”**, il +12% rispetto al 2019 e il +66% rispetto al 2017, per un danno economico e finanziario stimato due volte il PIL italiano, quindi intorno ai 3.500 miliardi di euro (4.300 miliardi di dollari circa).

Altre stime alzano l’asticella dei danni economici dovuti a cyber attacchi a oltre 6.000 miliardi di dollari entro la fine del 2021. Di fatto siamo di fronte ad una minaccia che cresce col passare del tempo e si estende a tutte le categorie produttive, industriali, aziendali, economiche e anche istituzionali, con le amministrazioni pubbliche nel mirino dei cyber criminali stabilmente ormai: nel 2020 gli attacchi alle strutture sanitarie sono il 12% del totale, mentre quelli rivolti alle amministrazioni centrali (ministeri/Governo, Difesa, Forze dell’Ordine e intelligence) arrivano al 14%.

Contrastare e neutralizzare questi attacchi è quindi fondamentale per le nostre imprese e industrie, ma anche per la Pubblica Amministrazione. Non si tratta più di qualcosa relegato al mondo immaginario di internet di qualche anno fa, gli attacchi informatici riguardano da vicino la nostra vita, la nostra quotidianità.

Nel mirino di chi attacca ci sono infrastrutture critiche, tra cui quelle energetiche e per le risorse idriche, quelle sanitarie e ospedaliere, e sappiamo bene quanto queste siano critiche per affrontare improvvisi crisi sanitarie come quella pandemica, fermare queste azioni criminali è centrale per la continuità di funzionamento del nostro sistema sociale prima ancora che economico.

Tecnologia “Shadow figment” e la guerra dei cloni ai cyber criminali

Scienziati del Pacific northwest national laboratory (**Pnnl**), del **Dipartimento dell’Energia del Governo degli Stati Uniti**, hanno sviluppato una nuova tecnologia anti-hacker/cracker chiamata “***Shadow figment***”.

La tecnologia è utilizzata per difendere obiettivi fisici, come le sopra citate infrastrutture critiche, ma anche edifici, servizi commerciali, reti di nuova generazione, fino alle fognature volendo, basata su soluzioni virtuali chiamate “***honeypot***”.

“*Honeypot*” è un sistema, o anche singola componente hardware/software, usato come “trappola” o “esca” a fini di protezione contro i cyber attacchi**. I ricercatori hanno messo a punto una specie di “sistema di cloni” delle infrastrutture critiche**, come la rete elettrica o idrica, ad esempio, che vengono attaccate dagli hacker, risparmiando quelle vere.

Fin dal 2015 abbiamo imparato a nostre spese quanto questi cyber attacchi siano pericolosi, come nel caso del blocco della rete elettrica in Ucraina, ma anche con l’attacco alla rete idrica in Florida negli Stati Uniti ad inizio anno, fino agli attacchi agli oleodotti della Colonial Pipeline, sempre negli Stati Uniti, e alla rete sanitaria nazionale irlandese delle ultime settimane.

Intelligenza artificiale e apprendimento automatico per forgiare i cloni delle infrastrutture critiche

Difficile dire se questa tecnica di distrazione

dell’attaccante sia efficace o meno. Gli studiosi del Pnnl sono convinti che la cartina di tornasole funzionerà, così da attirare i criminali verso obiettivi virtuali che non esistono, dei cloni appunto, facendogli credere di aver colpito il target.

La tecnologia in questione utilizza l’**intelligenza artificiale** per distribuire inganni sempre più elaborati, con lo scopo di mantenere gli aggressori impegnati con i cloni delle infrastrutture critiche. Una strategia di difesa frutto del lavoro delle unità di apprendimento automatico o ***machine learning***, che integrano nei cloni le conoscenze acquisite nel mondo reale attraverso i precedenti attacchi informatici alle infrastrutture critiche. In tal modo, chi attacca non dovrebbe accorgersi di avere a che fare con un obiettivo fittizio.

Se gli hacker attaccano una server farm virtuale (il clone di quella vera), con l’obiettivo di spegnere il sistema di aerazione, il team di “*Shadow figment*” rilasceranno segnali per indicare un aumento della temperatura interna alle sale, facendo credere che l’attacco è riuscito e che il danno si sta verificando (“*tidbits of success*”).

Non solo, tramite queste esche fittizie gli studiosi riescono anche a verificare che tipo di attacco è stato portato, con quali tecniche e quali danni, mentre nel frattempo si prova a mettere in campo diverse soluzioni di contrattacco e difesa, anche sperimentali.

Come dire, si sfruttano queste situazioni di crisi “controllata e pilotata”, tramite la tecnologia “*Shadow figment*”, anche per testare nuove armi di difesa informatica, anche perché, purtroppo, di soluzioni uniche e definitive contro il cyber crime non ce ne sono. La natura di questi attacchi è così mutevole e multiforme che anche le risposte devono essere all’altezza delle minacce.

https://www.key4biz.it/governo-usa-lancia-nuova-tecnologia-sha

dow-figment-una-guerra-dei-cloni-contro-i-cyber-criminali/363147/