# Phishing, 4500 nuovi domini fake a tema Covid e vaccini




Con l'arrivo delle prime dosi di vaccino contro il **Covid-19**, i ricercatori di sicurezza informatica di Webroot hanno dimostrato un aumento di termini e URL malevoli sul web.

In particolare le pagine fake riferite a vaccini, cure contro il COVID e alla possibilità di viaggiare, vengono sfruttate per colpire i soggetti più vulnerabili inducendoli ad aprire mail e link illeciti.

In particolare, la ricerca ha evidenziato:

- oltre **4.500** nuovi domini sospetti, contenenti una combinazione di termini relativi a "COVID-19", "Corona", "vaccino", "cure contro il COVID" e simili;
- **934** domini con lo specifico termine "vaccino" nel nome;
- **611** domini con errori di ortografia all'interno della parola "vaccino";

- **2.295** domini con il termine “COVID” nel nome;
- **622** domini con il termine “test” o suoi derivati nel nome;
- I nomi di alcuni domini sono risultati estremamente preoccupanti. Tra questi, “test per il COVID”, “aggiornamento sui test”, “passaporto COVID”, “vaccini privati”, ecc.

Inoltre, nel periodo tra l’8 dicembre e il 6 gennaio scorsi, l’azienda ha rilevato un **aumento nell’utilizzo della parola “vaccino”** all’interno di nomi di dominio sospetti pari al **336%** rispetto a marzo 2020, e al **94,8%** rispetto ai 30 giorni precedenti.

https://www.key4biz.it/covid-4500-nuovi-domini-fake-in-pochi-mesi/342626/

---

# Malware, la botnet Emotet non esiste più

**Emotet**, la botnet malware più grande al mondo, non esiste più. Grazie ad un’operazione internazionale coordinata dall’Europol e dall’Eurojust in collaborazione con le autorità giudiziarie di Germania, Paesi Bassi, Stati Uniti, Regno Unito, Francia, Lituania, Canada e Ucraina, uno dei servizi di criminalità informatica più professionali e duraturi in circolazione, è stato sconfitto.

## Emotet: la botnet attiva dal 2014

Apparsa in natura per la prima volta nel 2014, la botnet si è evoluta nel tempo fino a diventare un vero e proprio framework

criminale multi funzione. Emotet è un malware che si è diffuso nel corso degli anni passati prevalentemente tramite e-mail di phishing contenenti documenti Word infetti con un codice dannoso. Lo scopo di Emotet è quello installare una backdoor sui sistemi Windows così da renderli disponibili a vari scopi: distribuzione di ulteriore malware, ransomware e installazione di strumenti di accesso remoto.

# EMOTET takedown

EUROPOL

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

## Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

EUROPOL

## How did Emotet work?

### Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

### Installation

If victims opened the attachment or the link, the malware got installed.

### Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

## Emotet opened doors for:

- **Information stealers**
- **Trojans**
- **Ransomware**

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

## What made Emotet so dangerous?

| | |
|---|---|
| **Long lasting** | Started as a banking Trojan in 2014, evolving over time. |
| **Go-to-solution for criminals** | It acted as a door opener for other computers, allowing unauthorised access to other malware families. |
| **Polymorphic** | It changed its code each time it was called up. |
| **Resilient** | Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network. |

## Protect yourself from malware

**Always check your emails carefully and watch out for:**

- attachments or embedded links from unknown senders.
- messages with a sense of urgency asking you to download something.
- offers with a promise of reward that sounds too good to be true.

Fonte: Europol

## La collaborazione con i CSIRT

*“Per interrompere l’infrastruttura Emotet,* si legge nel comunicato dell’Europol, *le forze dell’ordine hanno collaborato per creare una strategia operativa efficace. Dato che l’infrastruttura utilizzata da Emotet ha coinvolto diverse centinaia di server dislocati in tutto il mondo, tutti dotati di funzionalità diverse per gestire i computer delle vittime infette, in un’operazione durata una settimana le forze dell’ordine e le autorità giudiziarie hanno acquisito il controllo dell’infrastruttura e l’hanno rimossa dall’interno. Le macchine infette delle vittime sono state reindirizzate verso questa infrastruttura controllata dalle forze dell’ordine”,* ha spiegato l’Europol. *“Un approccio nuovo e unico per interrompere efficacemente le attività dei facilitatori del crimine informatico”.*

L’Europol sta infine collaborando con i **Computer Emergency Response Team** (CSIRT) in tutto il mondo per aiutare coloro che hanno subito infezioni da parte di Emotet. L’indagine è comunque ancora in corso per l’identificazione dei responsabili e della loro gestione una volta individuati.

https://www.key4biz.it/malware-la-botnet-emotet-non-esiste-piu/341932/

---

# CSIRT, forze dell’ordine e

# magistratura. Come cooperare al meglio? Il report ENISA




L’Agenzia dell’Unione europea per la sicurezza informatica (**Enisa**) ha pubblicato un nuovo report per sostenere la cooperazione tra i **Computer Security Incident Response Team (CSIRT**), le forze dell’ordine e la magistratura.

Nel report dell’Enisa sono dettate le linee guida per aiutare ad affrontare le sfide di questa complessa cooperazione multi-stakeholder. Il rapporto, che comprende un manuale ed un set di strumenti per gli esperti, analizza ruoli, doveri, competenze, sinergie e potenziali interferenze tra i gruppi di

risposta agli incidenti di sicurezza informatica (CSIRT), in particolare quelli nazionali e governativi, le forze dll'ordine e magistratura (pubblici ministeri e giudici).

Il rapporto propone una metodologia per analizzare il quadro giuridico e organizzativo definendo i ruoli e i doveri, le competenze richieste dei CSIRT e delle forse dell'ordine. Identifica inoltre le sinergie e le potenziali interferenze che possono verificarsi durante le attività necessarie per rispondere a incidenti cyber e nella lotta alla criminalità informatica.

# Il CSIRT in Italia

In Italia il CSIRT è attivo dal 6 maggio 2020. 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.

# Per approfondire

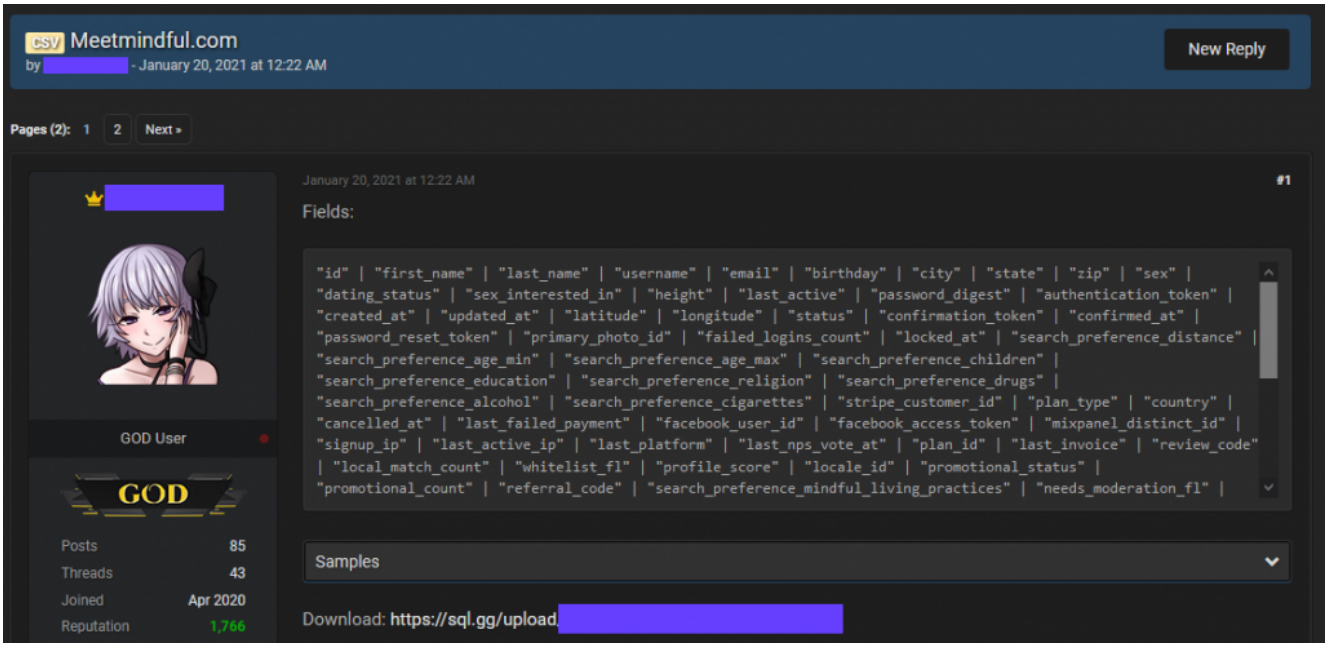
Clicca qui per scaricare il report Enisa **"2020 Report on CSIRT-LE Cooperation"**

https://www.key4biz.it/csirt-forze-dellordine-e-magistratura-come-cooperare-al-meglio-il-report-enisa/341722/

# Meetmindful, rubati i dati di 2,28 milioni di utenti (incluse le credenziali di Facebook)

Sono state rubate le informazioni di oltre 2,28 milioni di utenti registrati al sito di incontri **Meetmindful**. Tra questi, nomi, email, indirizzi, date di nascita, indirizzi IP, geolocalizzazioni, preferenze per gli appuntamenti e credenziali per entrare su **Facebook**.

Secondo il sito specializzato **ZDnet**, che ha riportato la notizia, i criminali informatici hanno condiviso un file da 1,2 Gb come download gratuito su un forum di hacking accessibile pubblicamente.



Fonte: Zdnet

Il contenuto di questo file include una grande quantità di informazioni fornite dagli utenti durante la configurazione

dei profili sul sito MeetMindful e sulle app per i dispositivi mobili, ma non i messaggi scambiati dagli utenti.

Il file trapelato è stato visualizzato più di 1.500 volte e molto probabilmente scaricato, osserva ZDnet. I dati sono stati rilasciati da **ShinyHunters**, un hacker che all'inizio di questa settimana ha anche fatto trapelare i dettagli di milioni di utenti registrati su **Teespring**, un portale che consente agli utenti di creare e vendere abbigliamento personalizzato.

## Allarme Sextortion

La fuga di dati dal sito **Meetmindful** rappresenta un grosso problema per gli utenti del sito e il motivo principale per cui **MeetMindful** deve informare i titolari degli account.

Il rischio infatti è che i criminali informatici possano usare i dati sottratti per attività illecite come il **Sextortion**, in cui i cyber criminali inviano email affermando di possedere informazioni compromettenti sul destinatario e minacciando la segnalazione a familiari o colleghi di lavoro.

https://www.key4biz.it/meetmindful-rubati-i-dati-di-228-milioni-di-utenti-incluse-le-credenziali-di-facebook/341294/

---

# Recovery plan, 8 milioni di euro per il Polo cibernetico di Roma




Nei piani del **Recovery plan** anche il nuovo **Polo cibernetico**. Nascerà a Roma in via **Tommaso Campanella**, in zona trionfale.

Il progetto, che rientra nel piano di investimenti per la Capitale, è di oltre 8 milioni di euro, grazie al recovery fund. Partito dal Ministero dell'Interno, il progetto prevede la riqualificazione di alcuni locali nello stesso immobile dove ha sede il Museo storico della **Polizia di Stato,** che sarà comunque preservato. Le operazione, si prevedono 1-2 anni di lavori, le seguirà come commissario **Vittorio Rapisarda**, provveditore interregionale delle opere pubbliche per il Lazio, l'Abruzzo e la Sardegna.

## Le funzioni del nuovo polo cibernetico

Il nuovo polo accoglierà la Direzione Centrale per la Sicurezza Cibernetica, articolazione che nel processo di riorganizzazione del Dipartimento della Pubblica Sicurezza è destinata ad assorbire le funzioni e le attribuzioni dell'attuale Servizio di Polizia Postale e delle Comunicazioni.

La futura Direzione Centrale avrà principalmente compiti di prevenzione, contrasto e repressione dei crimini informatici e sarà suddivisa in tre servizi: uno di tipo amministrativo per gli affari generali e due operativi. Il primo gestirà il contrasto ai fenomeni del cyber bullismo, del sexting e più in generale i delitti che vedono coinvolte le cosiddette "fasce deboli", il secondo conterrà proprio il *"Computer Security Incident Response Team"* **(Csirt Italia),** ex **C.E.R.T,** il nuovo team dello per gestire la cyber-difesa nazionale italiana istituito presso il Dipartimento Informazioni per la Sicurezza (**DIS**).

# Cybersecurity: in Italia anche le aziende sono ad alto rischio informatico

Non soltanto cyberwar e frodi informatiche che coinvolgono gli utenti. Nell'ultimo report "Cyber Risk Index (CRI)" elaborato da Trend Micro, in collaborazione con il Ponemon Institute, anche le aziende italiane sono considerate a "rischio elevato" di subire un attacco o una violazione e hanno basse capacità di reazione.

Lo studio ha l'obiettivo di approfondire i livelli di rischio legati alla cybersecurity nelle aziende di tutto il mondo e mappare lo scenario attuale attraverso la creazione del Cyber Risk Index (CRI), indicatore che calcolando il divario tra le difese cyber dell'azienda, ovvero la postura di sicurezza, e la possibilità di subire un attacco, è in grado di predire il rischio di subire gravi danni cyber in una determinata area.

Il Cyber Risk Index si basa su una scala numerica che va da "-10" a "10" con il valore "-10" che rappresenta il rischio più alto. La scala di rischio è composta da "rischio basso", (verde) "rischio moderato" (giallo), "rischio elevato" (arancione) e "rischio alto" (rosso).

Il Cyber Risk Index globale attuale è di “-0,41”, ovvero rischio elevato. L’area con il rischio maggiore è quella degli Stati Uniti, con un Cyber Risk Index di “-1,07”, mentre sia in Europa che in Italia il valore si attesta a “-0,13” indicando un “rischio elevato”.

La regione più virtuosa è quella asiatica, con un Cyber Risk Index che misura “-0,02”. Le aziende che si trovano in un’area a “rischio elevato” si caratterizzano per l’alta possibilità di subire una compromissione di dati, una scarsa visibilità delle minacce all’interno delle reti e la mancanza di una procedura di gestione e reazione agli incidenti. Rispetto all’Italia, altri Paesi in Europa sono più virtuosi, come per esempio Germania e UK che hanno un rischio moderato e sono classificate come zona gialla.

https://www.key4biz.it/recovery-fund-8-milioni-di-euro-per-il-polo-cibernetico/340830/

---

# L’azienda di sicurezza informatica Malwarebytes è stata violata dagli hacker di SolarWinds




Lo stesso gruppo che ha violato la società di software IT **SolarWinds** lo scorso dicembre ha violato la società di sicurezza informatica americana **Malwarebytes**.

Lo riporta la stessa azienda californiana in un post scritto dal CEO dell'azienda di cybersecurity **Marcin Kleczynski**.

*"Malwarebytes ha appreso della violazione il 15 dicembre dal Microsoft Security Response Center e da allora ha indagato sulla questione",* scrive il CEO. *"I Criminali informatici hanno avuto accesso solo ad un numero limitato di e-mail aziendali interne*", aggiungendo che *"il software dell'azienda resta sicuro da usare".*

Malwarebytes ha affermato che gli hacker hanno utilizzato una debolezza in **Azure Active Directory** e applicazioni dannose di **Microsoft Office 365** per violare i sistemi interni dell'azienda. Inoltre l'hackeraggio non è correlato alla violazione dei software SolarWinds, poiché Malwarebytes non utilizza nessuno dei loro sistemi.

# 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.

> *Today, I disclosed publicly that @Malwarebytes had been targeted by the same nation state actor that attacked SolarWinds. This attack is much broader than SolarWinds and I expect more companies will come forward soon.*
>
> *— Marcin Kleczynski (@mkleczynski) January 19, 2021*

In un messaggio pubblicato su Twitter, **Kleczynski** ha affermato che la campagna di hacking che ha coinvolto SolarWinds *"è molto più ampia e mi aspetto che altre aziende si facciano avanti presto".*

https://www.key4biz.it/lazienda-di-sicurezza-informatica-malwarebytes-e-stata-violata-dagli-hacker-di-solarwinds/340352/

# Cloud e cybersecurity, l’Enisa presenta le linee guida per il settore sanitario



L’Agenzia dell’Unione europea per la sicurezza informatica (**Enisa**) ha pubblicato un nuovo report che fornisce linee guida sulla sicurezza informatica per le organizzazioni sanitarie, per aiutarle a digitalizzare ulteriormente con i servizi cloud.

***“Cloud Security for Healthcare Services”*** valuta i rischi per la sicurezza informatica dei servizi cloud e offre buone pratiche per la loro integrazione nel settore sanitario

europeo. Il nuovo report arriva mentre la Commissione europea sta portando avanti quest'anno l'iniziativa **European Health Data Space** per promuovere lo scambio sicuro dei dati dei pazienti e l'accesso ai dati sanitari.

# Cloud e cybersecurity: le linee guida del report

Basandosi sulle linee guida per gli appalti di Enisa per la sicurezza informatica negli ospedali, pubblicate all'inizio del 2020, il rapporto affronta le preoccupazioni precedenti fornendo linee guida sulla sicurezza per tre aree principali in cui i servizi cloud sono utilizzati dal settore sanitario, vale a dire per:

- **Electronic Health Record** (EHR) , o sistemi incentrati sulla raccolta, l'archiviazione, la gestione e la trasmissione di dati sanitari, quali informazioni sui pazienti e risultati di esami medici;
- **Remote Care**, o il sottoinsieme della telemedicina che supporta la consultazione remota paziente-medico;
- **Servizi cloud** che supportano il funzionamento di dispositivi medici a diverse parti interessate

Per ciascuno di questi casi d'uso, il report evidenzia i principali fattori da considerare quando le organizzazioni sanitarie conducono la relativa valutazione del rischio. Queste linee guida, tuttavia, sono solo un primo passo per gli operatori sanitari per adattarsi in modo sicuro al cloud. Enisa ha affermato che è necessario un maggiore supporto, come standard di settore stabiliti sulla sicurezza del cloud, indicazioni specifiche delle autorità nazionali e dell'UE e ulteriori linee guida delle autorità per la protezione dei dati sul trasferimento dei dati sanitari nel cloud.

Il rapporto propone inoltre una serie di misure di sicurezza che le organizzazioni sanitarie devono implementare quando

pianificano il passaggio ai servizi cloud, come stabilire processi per la gestione degli incidenti, definire i requisiti di crittografia dei dati e garantire la portabilità e l'interoperabilità dei dati.

## Per approfondire

https://www.key4biz.it/cloud-e-cybersecurity-lenisa-presenta-le-linee-guida-per-il-settore-sanitario/340155/

---

# Phishing, Polizia Postale: "In Italia falsi rimborsi Enel truffano gli utenti"

La **Polizia Postale** ha avvisato gli utenti che è in atto una nuova mail-truffa che sfrutta l'immagine contraffatta di **Enel**, la multinazionale leader che produce e distribuisce energia elettrica e gas.

*"Dopo i calcoli finali della tua bolletta Enel energia, abbiamo stabilito che sei idoneo a ricevere un rimborso dell'importo di 128,04 euro. Un'altra truffa mascherata da "rimborso" per ingannare gli utenti,* spiega la Polizia Postale attraverso un comunicato, *invitando utenti e cittadini a non cliccare o scaricare nessun documento.*




Fonte: commissariatodips.it

*“Un consiglio da seguire per non cadere vittime della truffa, è quello di non aprire assolutamente la mail e di contattare telefonicamente l’Enel attraverso il numero verde così da richiedere un controllo e verificare realmente la veridicità dei fatti”,* spiega la nota.

# Brand Phishing in aumento

Questa tipologia di attacchi sono sempre più numerosi e coinvolgono aziende e multinazionali famose: Brand Phishing.

In un attacco di brand phishing, i criminali cercano di imitare il sito web ufficiale di un'azienda nota, utilizzando un nome di dominio o un URL e un design web simile a quello del sito originale. Il link al sito web falso può essere inviato a individui mirati tramite e-mail o SMS, oppure un utente può essere reindirizzato durante la navigazione sul web o può essere attivato da un'applicazione mobile fraudolenta. Il sito web falso spesso contiene un modulo destinato a rubare le credenziali degli utenti, i dati di pagamento o altre informazioni personali.

Secondo un recente report di sicurezza informatica, **Microsoft** e **DHL** sono le multinazionali più sfruttate in quanto i cyber criminali cercano di sfruttare l'aumento del lavoro da casa e la stagione degli acquisti online.

Nel quarto trimestre, Microsoft è stato ancora il brand più frequentemente sfruttata dai criminali informatici. Il 43 per cento di tutti i tentativi di brand phishing sono collegati al gigante della tecnologia (con un balzo rispetto al 19 per cento nel terzo trimestre), dato che gli hacker gli hanno continuato a cercare di approfittarsi delle persone che lavorano da remoto.

L'industria che più è stata presa di mira dal brand phishing è quella IT, seguita dalle spedizioni, dalla vendita al dettaglio all'energia.

https://www.key4biz.it/phishing-polizia-postale-in-italia-falsi-rimborsi-enel-truffano-gli-utenti/339705/

# Anne Neuberger a capo della sicurezza informatica degli Stati Uniti



Il presidente eletto **Joe Biden** ha nominato **Anne Neuberger** vice consigliere per la sicurezza nazionale e responsabile della sicurezza informatica.

Lo riporta Politico.com Neuberger, attuale capo della divisione per la sicurezza informatica della National Security Agency (Nsa), avrà il compito di coordinare la sicurezza informatica per il governo federale degli Stati Uniti. Non solo.

Fra le proprietà di Neuberger vi sarà anche la massiccia campagna di spionaggio informatico durata mesi che ha compromesso decine di agenzie governative statunitensi e aziende private. I funzionari statunitensi sospettano che dietro l'attacco ci siano hacker russi.

# Anne Neuberger: il profilo

Ebrea ortodossa, 45 anni, Neuberger, vanta un curriculum di oltre un decennio presso la Nsa.

Laureata presso il Touro College nel 1997 Neuberger si è laureata alla Columbia University con un master in amministrazione aziendale e un master in affari internazionali nel 2005. Entrò nel governo come borsista della Casa Bianca, lavorando per il Segretario alla Difesa e poi servì come Vice Direttore Generale della Marina.

Neuberger è entrata a far parte della National Security Agency (NSA) nel 2009 e ha ricoperto posizioni chiave prima del suo ruolo attuale. Ha contribuito a stabilire il Cyber Command degli Stati Uniti e ha lavorato come chief risk officer, guidando gli sforzi per la sicurezza elettorale dell'agenzia per le midterm del 2018.

Nel 2019, il generale **Nakasone** ha costituito la direzione della sicurezza informatica della NSA e ha nominato Neuberger il primo direttore della sicurezza informatica. La direzione si concentra sulla "prevenzione e l'eliminazione" delle minacce informatiche da Paesi come Russia, Cina, Iran e Corea del Nord.

https://www.key4biz.it/una-donna-a-capo-della-sicurezza-informatica-degli-stati-uniti/339586/

---

# Parler, hackerati 56,7

# terabyte di dati prima della chiusura del sito




Doveva essere il momento della svolta per **Parler**, il social sovranista che piace tanto ai seguaci di Trump. E invece nell'arco di due giorni è stato quasi annientato.

Prima **Google** e **Apple** hanno rimosso l'app della piattaforma dai loro store digitali poco prima che **Amazon** staccasse la spina ai server lasciando di fatto il sito offline per tutti i seguaci di Trump e gli altri utenti iscritti.

Infine il colpo di grazia. Una ricercatrice informatica è riuscita infatti a scaricare tutto il social network, quindi ogni singolo messaggio e profilo dal portale, comprese informazioni potenzialmente incriminanti come ad esempio fotografie degli assalti al Congresso scattate il 6 gennaio, pubblicate sul sito e già cancellate poco prima che Amazon chiudesse forzatamente i battenti.

# L’hacker Donk_enby

L’hacker che ha compiuto il gesto, donk_enby, una ragazza di 26 anni, è stata in grado di acquisire e archiviare quasi l’intero contenuto del sito Web, circa 56,7 terabyte, dopo che centinaia di sostenitori di Trump avevano caricato foto e video potenzialmente incriminanti di se stessi sulla piattaforma, riprese dall’interno del Campidoglio stesso durante l’assalto del 6 gennaio.

Quando le voci sull’imminente cancellazione di Parler hanno cominciato a circolare, donk_enby, che ha fatto ricerche su Parler per mesi, ha capito che una litania di informazioni importanti sui più importanti gruppi estremisti di estrema destra d’America rischiava di essere permanentemente nascosta agli occhi del pubblico.

*“Tutto ciò che abbiamo acquisito era pubblicamente disponibile sul Web, ne abbiamo semplicemente creato un’istantanea pubblica permanente*“, ha commentato donk_enby in un’intervista al sito Vice.com.

*“Con l’FBI, le forze dell’ordine statali e locali e gli investigatori open source che cercano i responsabili dell’attacco di mercoledì, l’archivio potrebbe essere molto utile per un’intera schiera di persone”,* ha dichiarato Donk_emby.

*“Spero che l’archivio possa essere utilizzato per ritenere le persone responsabili e per prevenire ulteriori morti”,* ha detto. *“Penso che alle persone dovrebbe essere consentito di avere la propria opinione fintanto che possono agire in modo civile, mercoledì abbiamo visto cosa può accadere se non lo fanno”.*

# La scarsa sicurezza di Parler

Usando un iPad e **Ghidra**, un software di reverse engineering progettato e rilasciato pubblicamente dalla National Security Agency, donk_enby è riuscita a sfruttare i punti deboli nel design del sito web per estrarre gli URL di ogni singolo post pubblico su Parler in ordine sequenziale, dal primo all'ultimo, permettendole di catturare e archiviare i contenuti.

Donk_enby aveva originariamente inteso acquisire dati solo dal giorno dell'acquisizione del Campidoglio, ma ha scoperto che la **scarsa costruzione e sicurezza di Parler le hanno permesso di acquisire, essenzialmente, l'intero sito web.**

Alla fine sono stati 56,7 terabyte di dati, che includevano ogni post pubblico su Parler, 412 milioni di file in tutto, inclusi 150 milioni di foto e più di 1 milione di video.

Ognuno di questi aveva metadati incorporati come data, ora e coordinate GPS: a differenza della maggior parte dei siti di social media, Parler non elimina i metadati dai media caricati dagli utenti, il che, soprattutto, potrebbe essere utile per le forze dell'ordine e gli investigatori open source.

I dati sono attualmente in fase di elaborazione e dovrebbero essere disponibili per la navigazione tra un paio di giorni, secondo donk_enby. I primi archivi di esso stanno già spuntando come file torrent e vengono condivisi su canali IRC e diversi siti git.

https://www.key4biz.it/parler-hackerati-567-terabyte-di-dati-prima-della-chiusura-del-sito/339188/