Investigator Says Amazon Chief’s Phone Hacked by Saudis

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/lSJeC7qGQkw/investigator-says-amazon-chiefs-phone-hacked-saudis

---

Georgia Man Admits to Hacking Accounts of Athletes and Musicians

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/vddpzj1YsL4/georgia-man-admits-hacking-accounts-athletes-and-musicians

---

Millions of Toyota Customers in Japan Hit by Data Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/sPmSHUDue4I/millions-toyota-customers-japan-hit-data-breach

Ex-NSA Contractor Pleads Guilty in Theft of Secret Documents

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/uj7i_VIDtI4/ex-nsa-contractor-pleads-guilty-theft-secret-documents

---

Ex-NSA Contractor Expected to Plead Guilty in Document Theft

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ayqYhdbWiKA/ex-nsa-contractor-expected-plead-guilty-document-theft

---

WinRAR Vulnerability Exploited to Deliver New

Malware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_hIciDMeQ9s/winrar-vulnerability-exploited-deliver-new-malware

---

Cloud e data center nel mirino degli hacker. In aumento attacchi DDoS a livello globale

La digital transformation è una strategia fondamentale per le aziende che intendono cogliere nuove opportunità di guadagno, ma fa sì che questi nuovi servizi attirano l'attenzione dei criminali informatici, che hanno iniziato a colpirli con sempre maggiore frequenza.

A dirlo è il rapporto annuale sulla sicurezza delle infrastrutture mondiali di **Netscout,** giunto alla quattordicesima edizione, un documento che contiene importanti informazioni sulle sfide operative e di sicurezza affrontate dai service provider e dagli operatori delle reti aziendali in diversi paesi del mondo.

Secondo lo studio a farla da padrone sono gli attacchi **DDoS** (***Denial of Service),*** attacchi informatici in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio ai client richiedenti.

Nel 2018, spiega il report, l’entità degli attacchi DDoS ha subito un’impennata raggiungendo il livello record di 1,7 Tbps, mentre continuano a evolversi nuovi bersagli e nuove tecniche.

Gli attacchi DDoS continuano a crescere

Il report in particolar modo evidenzia:

- Il 91% delle aziende colpite da un attacco DDoS ha dichiarato che uno o più attacchi hanno saturato completamente la banda Internet.
- I criminali informatici si sono concentrati maggiormente sugli attacchi alle infrastrutture stateful, colpendo firewall e dispositivi IPS. Questi attacchi sono quasi raddoppiati, passando dal 16 al 31%.
- Tra i soggetti colpiti dagli attacchi stateful, il 43% ha riferito che il firewall e/o il dispositivo IPS ha contribuito a un’interruzione durante l’attacco.
- Il 36% delle aziende ha subito attacchi multivettore complessi mirati alla banda, all’infrastruttura stateful e alle applicazioni.

Gli ingenti costi dei tempi di inattività

Nel 2018, il costo globale medio di un’ora di inattività associata alle interruzioni dei servizi Internet causate dagli attacchi DDoS ammontava a 221.836,80 dollari. Il costo più elevato, registrato in Germania, corrisponde a 351.995 dollari. In Giappone, un’ora di inattività della rete ammonta

invece a 123.026 dollari.

Chi sono le vittime preferite del cybercrime

- **Servizi SaaS**

Gli attacchi DDoS contro i servizi SaaS sono triplicati rispetto all’anno precedente, passando dal 13 al 41%.

- **Data center e servizi cloud esterni**

Anche in questo settore, gli attacchi DDoS sono triplicati rispetto all’anno precedente, passando dall’11 al 34%.

- **Attacchi al traffico crittografato**

Il crescente utilizzo del traffico crittografato si riflette nella maggiore percentuale di attacchi mirati contro questo tipo di traffico. Nel 2018, il 94% degli intervistati ha osservato attacchi di questo genere, in quantità quasi raddoppiate rispetto all’anno precedente.

- **Service provider**

Anche i servizi basati su cloud sono stati maggiormente colpiti dagli attacchi DDoS, con un aumento dal 25% del 2016 al 47% del 2018.

https://www.key4biz.it/cloud-e-data-center-nel-mirino-degli-hacker-in-aumento-attacchi-ddos-a-livello-globale/251659/

Virus Melissa: 20 anni dopo cosa abbiamo imparato?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*

Il 26 marzo del 1999 iniziò a diffondersi un virus, creato da un tale **David Lee Smith**, che infettò oltre 1 milione di sistemi; provocò danni diretti stimati in oltre 80 milioni di dollari e bloccò, anche per diversi giorni, l'operatività dei server mail di oltre 300 grandi aziende ed enti governativi.

Il programmatore Smith, ammiratore della bella striptease Melissa, prese possesso di un *account* di AOL e lo utilizzò per pubblicare un file in un gruppo Internet chiamato "alt.sex", promettendo decine di password per accessi gratuiti a siti che forniscono materiale non idoneo per i minori. Una volta aperto il documento Word, il virus si diffondeva nel computer e quindi, utilizzando Outlook, si spediva agli indirizzi email trovati. La email spedita suggeriva al destinatario di aprire il documento allegato che aveva un nome del tipo "sexxxy.jpg" oppure "naked wife".

Già 20 anni fa il phishing sfruttava anche email inviate da persone conosciute!

La velocità di propagazione e i problemi creati misero in allarme l'FBI che sollecitò tutti a porre attenzione alle email ed ai relativi allegati.

Fu questo il primo episodio di una certa gravità? No.

Un grave episodio era già avvenuto 11 anni prima! Infatti, il

2 novembre del 1988 un worm (conosciuto come **Morris worm**) si diffuse su Internet: nelle prime 24 ore aveva già bloccato circa il 10% dei computer connessi in rete. Colpiti furono i sistemi UNIX del Massachusetts Institute of Technology (MIT), e di Harvard, Princeton, Stanford, Johns Hopkins, NASA, ed il Lawrence Livermore National Laboratory.

Oltre a sfruttare una porta ed un problema nel software di identificazione degli utenti in rete, era progettato anche per stare nascosto.

Domanda: gli utilizzatori hanno finalmente compreso la lezione?

Scrive il CLUSIT:«*Tutti gli analisti ed esperti di sicurezza concordano* ***che la maggior parte degli incidenti di sicurezza è legata ad errori umani*** *(si stima che siano circa l'80%-90% degli incidenti) confermando come il fattore umano sia, anche per la sicurezza informatica, l'anello debole del sistema. Solo in Italia si è stimato che circa il 53% degli attacchi sono dovuti a cause endogene (****utilizzo di password deboli e non alfanumeriche, accesso di device aziendali a connessioni pubbliche, navigazione in siti non sicuri e il trasporto di dati sensibili con chiavi USB non cifrate****,…) e a queste si sommano gli attacchi di phishing e spear phishing che provocano impatti significativi sull'azienda sia in termini di frodi e dati rubati che come incremento dei costi operativi per il ripristino dagli incidenti occorsi*.».

Conclusione: 1988, 1999, 2019: nulla è cambiato nell'atteggiamento del cittadino?

Vi è però, a mio parere, una eccezione che fa piacere. Nell'ambito della mia attività presso l'AGID mi è capitato di leggere la esigenza, manifestata dal management di diversi Enti della Pubblica Amministrazione, di far frequentare corsi di sensibilizzazione ad attacchi di Social Engineering a tutto il personale, IT incluso. Ottimo!

Ma ciò a mio parere non basta, in quanto bisogna far sì che l’attenzione alle minacce entri nel DNA delle persone.

Che fare quindi?

La soluzione a mio parere è di iniziare a **diffondere la cultura dell’attenzione ai rischi iniziando dai ragazzi, se non addirittura dai più piccoli.**

Nel prossimo articolo racconterò della mia esperienza con decine di classi medie inferiori in due regioni italiane.

Anthony Cecil Wright

https://www.key4biz.it/virus-melissa-20-anni-dopo-cosa-abbiamo-imparato/251563/

Microsoft Takes Control of 99 Domains Used by Iranian Cyberspies

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/a2GnUGynQzg/microsoft-takes-control-99-domains-used-iranian-cyberspies

---

Iran-Linked Cyberspy Group APT33 Continues Attacks on Saudi Arabia, U.S.

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/cgUVocgebm4/iran-linked-cyberspy-group-apt33-continues-attacks-saudi-arabia-us