Usa-Iran, un conflitto anche cibernetico? I 5 possibili cyber attacchi

Gli Stati Uniti e l'Iran sono due delle potenze di hacking più avanzate, attive e capaci al mondo in un momento in cui i governi usano regolarmente gli attacchi informatici per raggiungere importanti obiettivi e modellare la geopolitica. Le tensioni tra i due Paesi e i loro alleati hanno prodotto una lunga storia di straordinari cyber attacchi oltre alla tradizionale guerra cinetica. Per questi motivi la vendetta dell'Iran per l'uccisione del generale **Qassim Suleimani** potrebbe essere servita agli Stati Uniti anche sul terreno del cyberspazio.

Christopher Krebs, direttore della Cybersecurity and Infrastructure Security Agency (**CISA**) del dipartimento della sicurezza nazionale Usa, ha avvisato tutta la comunità di studiare nuovamente in modo dettagliato le tattiche, procedure e tecniche (TTP) di Teheran nel cyberspazio, dopo aver comunicato l'aumento delle attività di attacchi informatici malevoli diretti alle aziende e alle agenzie governative degli Stati Uniti.
"Gli hacker del regime iraniano", ha spiegato Krebs*, "usano sempre più attacchi distruttivi a 'tergicristalli'".* Come:

- *spear phishing*, la truffa via email per ottenere accesso non autorizzato ai dati sensibili.
- *password spray*: l'hacker tenta una password utente comune su più account prima di passare a una seconda password che consente di eludere i blocchi degli account.

- *credential stuffing, s*i tratta di un attacco che fa leva sulla probabilità che le persone possano utilizzare lo stesso nome utente e la stessa password per accedere a più applicazioni, siti e servizi. I cybercriminali acquisiscono i dettagli degli account rubati da una piattaforma e implementano i bot necessari per accedere a molti altri account con le stesse credenziali. Una volta trovato il modo di accedere, i criminali violeranno l'account, effettuando acquisti fraudolenti o sottraendo informazioni riservate.

Prima che l'accordo nucleare del 2015 fosse negoziato tra Stati Uniti, Iran, Europa, Russia e Cina, gli hacker iraniani prendevano regolarmente di mira le società finanziarie americane e le infrastrutture critiche.

Nell'ultimo anno, l'Iran e gli Stati Uniti si sono ripetutamente presi di mira a vicenda nelle operazioni di pirateria informatica. Gli hacker del governo iraniano hanno tentato di violare la campagna di rielezione del presidente Trump. Secondo quanto riferito, il Cyber □□Command statunitense ha ostacolato la forza paramilitare dell'Iran durante un periodo di forti tensioni all'inizio di quest'anno.

150 siti americani già vittime di defacement da parte di hacker iraniani

La guida suprema, l'ayatollah **Ali Khamenei**, ha promesso "una forte vendetta" per l'uccisione di **Suleimani** e trattandosi di un conflitto moderno, ad oggi solo minacciato, non potrebbe che essere anche una guerra cibernetica. I 150 i siti americani finora defacciati dai sostenitori del regime degli Ayatollah sono solo un avvertimento?

Nei giorni scorsi, gli hacker vicini a Teheran hanno bucato il sito del Federal Depository Library Program (**FDLP**) con

un’operazione appunto di *defacement*, lasciando un messaggio in cui affermano che “*questa è solo una piccola parte delle capacità cyber iraniane”.* L’attacco ha preso di mira un bersaglio “debole”, ma è un segnale che il cyber army della Repubblica islamica è stato attivato per colpire obiettivi legati agli Usa. In particolare le infrastrutture critiche.

I 5 possibili cyber attacchi dell’Iran

Jon Bateman, senior intelligence analyst per l’Iran presso la **Defence Intelligence Agency**, citato da **Fifth Domain**, ritiene che le aggressioni potrebbero avvenire in cinque modalità:

- attacchi DDoS, in cui si inonda un sito di richieste di accesso mandandolo in crash.
- data deletion (o wiper attack), azioni tese alla cancellazione dei dati nei database infettati.
- attacchi ai sistemi di controllo industriali (ICS), operazioni legate alle informazioni e nonché spionaggio cibernetico.

Questi ultimi due per rubare dati da impiegare poi in azioni militari “fisiche”. Per esempio commettere omicidi mirati o attacchi contro infrastrutture.

Ma la Repubblica islamica potrebbe subire dalla reazione americana molti più danni di quelli che potrebbe causare. È già successo in passato, come confermato dallo stesso capo della “cyber polizia” di Teheran, il generale **Kamal Hadianfar**, che ha ammesso che l’Iran nel 2017 ha subìto 296 cyber aggressioni gravi contro le infrastrutture vitali e in più occasioni esperti del settore sono morti misteriosamente.

> *Usa-Iran, un conflitto anche cibernetico? I 5 possibili cyber attacchi*

More Than 150,000 U.S. Small-Business Websites Could Be Infected With Malware at Any Given Moment. Here’s How to Protect Yours.

Small-business victims were involved in 43 percent of data breaches over the course of a year, according to a recent report.

December 27, 2019 9 min read

It was March 2, 2016, and Melissa Marchand’s day on Cape Cod started out like any other. She drove to her job at Hyannis Whale Watcher Cruises in her mid-size sedan, picked up a latte with 1 percent milk at her local coffee shop and sat down at her desk to check her email. Then, Marchand got the call no website manager ever wants to receive: The site was down, and no one knew how to fix it.

After she dialed up the web hosting provider, the news went from bad to worse: Whales.net had been hacked and, to her horror, all visitors were being redirected to porn sites. Google had even flagged the company’s search results, warning potential customers that the site may be hacked.

“It was a total nightmare – I had no idea that something like this could happen,” Marchand said in an interview with

Entrepreneur. “I’d say 75 to 80 percent of our bookings are done online, so when our site is down, we’re just dead in the water.”

At the provider’s suggestion, Marchand called SiteLock, a website security company, and granted its representatives site access. SiteLock discovered the hackers had exploited a security hole in a WordPress plugin, which gave them the access they needed to redirect visitors to racy websites.

By the end of the work day, Marchand sat in her car in her gym’s parking lot, speaking on the phone with a SiteLock representative to review the plan of action. She finally felt like things were going to be OK.

Within three days, Whales.net was back up and running, though it took another three weeks for Google to remove the blacklist warning from the company’s search results.

The hack hit about a month before the whale-watching season began in mid-April, and though it wasn’t peak season, the company still missed out on pre-booking tour groups from schools and camps. Marchand estimated the attack lost the company about 10 percent of its March and April business.

A risk for small businesses everywhere

Small-business owners were victims in 43 percent of data breaches tracked between Nov. 1, 2017, and Oct. 31, 2018, according to a 2019 Verizon report. The report tracked security incidents across all industries, but the most vulnerable sectors this year were retail, accommodation and healthcare.

What does the issue look like on a national scale? If we take the sample size of infected sites SiteLock said they found in 2018 — approximately 47,244 out of 6,056,969 checked — and

apply that percentage to the country's estimated 30.2 million small-businesses websites, minus the estimated 36 percent that don't have one, then we can loosely estimate the amount of infected small-business websites to be around 150,757.

As a small-business owner, you may not believe anyone would target your website, but that's just it – bad actors are likely not seeking out your site specifically, said Mark Risher, head of account security at Google.

"Sometimes, we talk about the distinction between targets of choice and targets of chance," Risher said. "Targets of chance is when the attacker is just trying anything – they're walking through the parking lot seeing if any of the car doors unlocked. Target of choice is when they've zeroed in on that one shiny, flashy car, and that's the one they want to break into – and they'll try the windows, the doors … the moon roof. I think for small businesses, there's this temptation to assume, 'No one would ever choose me; therefore I'll just kind of skate by anonymously.' But the problem is they're not factoring in the degree of automation that attackers are using."

Even the least-trafficked websites still average 62 attacks per day, according to SiteLock research. "These cybercriminals are really running businesses now," said Neill Feather, president of the company. "With the increasing ease of automation of attacks, it's just as lucrative to compromise a 1,000 small websites as it is to invest your time and try to compromise one large one."

John Loveland, a cybersecurity head at Verizon and one of the data breach report's authors, said that since the report was first published 12 years ago, he's seen a definite uptick in attacks at small and medium-sized businesses. As malware, phishing and other attacks have become "more commoditized and more readily accessible to lesser-skilled hackers," he said, "you see the aperture open … for types of targets that could

be valuable.”

So what are the hackers getting out of the deal? It’s not just about potentially lucrative customer information and transaction histories. There’s also the opportunity to weaponize your website’s reputation. By hosting malware on a formerly trustworthy website, a hacker can increase an attack’s spread – and amplify the consequences – by boosting the malware’s search engine optimization (SEO). They can infect site visitors who search for the site organically or who access it via links from newsletters, articles or other businesses, Risher said.

Even if you outsource aspects of your business – say, time and expense reporting, human resources, customer data storage or financial transactions – there’s still no guarantee that that information is safe when your own website is compromised. Loveland said he saw an uptick in email phishing specifically designed to capture user credentials for web-based email accounts, online CRM tools and other platforms – and reports of credential compromise have increased 280 percent since 2016, according to an annual survey from software company Proofpoint.

How to protect yourself and your customers

How can small-business owners protect themselves – and their customers? Since a great deal of cyberattacks can be attributed to automation, putting basic protections in place against phishing, malware and more can help your site stay off the path of least resistance.

Here are five ways to boost your small-business’s cybersecurity.

1. Use a password manager.

There’s an exhaustive amount of password advice floating around in the ether, but the most important is this, Risher said: Don’t reuse the same password on multiple sites. It’s a difficult rule to stick to for convenience’s sake – especially since 86 percent of internet users report keeping track of their passwords via memorization – but cybersecurity experts recommend password managers as efficient and secure workarounds. Free password manager options include LastPass, Myki and LogMeOnce.

2. Set up email account recovery methods to protect against phishing attacks.

Phishing attacks are an enduring cybersecurity problem for large and small businesses alike: 83 percent of respondents to Proofpoint’s annual phishing survey reported experiencing phishing attacks in 2018, an increase from 76 percent the year before. Embracing a more cyber-aware culture – including staying vigilant about identifying potential phishing attacks, suspicious links and bogus senders – is key to email safety.

If you’re a Gmail user, recent company research suggests that adding a recovery phone number to your account could block up to 100 percent of cyberattacks from automated bots, 99 percent of bulk phishing attacks and 66 percent of targeted attacks. It’s helpful because in the event of an unknown or suspicious sign-in, your phone will receive either an SMS code or an on-device prompt for verification. Without a recovery phone number, Google will rely on weaker challenges such as recalling last sign-in location – and while that still stops most automated attacks, effectiveness against phishing drops to 10 percent.

3. Back up your data to protect against ransomware.

Ransomware – a cyberattack in which a hacker holds your computer access and/or data for ransom – has kicked off a "frenzy of cybercrime-related activities focused on small and medium businesses," Loveland said. In fact, it's the second leading malware action variety in 2019, according to the Verizon report, and accounted for 24 percent of security incidents. Hackers generally view it as a potentially low-risk, high-reward option, so it's important to have protections in place for such an attack – namely, have your data backed up in its entirety so that you aren't at the hacker's mercy. Tools such as Google Drive and Dropbox can help, as well as automatic backup programs such as Code42 (all charge a monthly fee). You can also purchase a high-storage external hard drive to back everything up yourself.

4. Enlist a dedicated DNS security tool to block suspicious sites.

Since computers can only communicate using numbers, the Domain Name System (DNS) is part of the internet's foundation in that it acts as a "translator" between a domain name you enter and a resulting IP address. DNS wasn't originally designed with top-level security in mind, so using a DNSSEC (DNS Security Extension) can help protect against suspicious websites and redirects resulting from malware, phishing attacks and more. The tools verify the validity of a site multiple times during your domain lookup process. And though internet service providers generally provide some level of DNS security, experts say using a dedicated DNSSEC tool is more effective – and free options include OpenDNS and Quad9 DNS. "[It's] a low-cost, no-brainer move that can prevent folks from going to bad IP addresses," Loveland said.

5. Consider signing up with a website security company.

Paying a monthly subscription to a website security company may not be ideal, but it could end up paying for itself in terms of lost business due to a site hack. Decreasing attack vulnerability means installing security patches and updates for all of your online tools as promptly as possible, which can be tough for a small-business owner's schedule.

"It's tempting for a small-business owner to say, 'I'm pretty handy – I can do this myself,'" Risher said. "But the reality is that even if you're very technical, you might not be working around the clock, and … you're taking on 24/7 maintenance and monitoring. It's certainly money well spent to have a large organization doing this for you."

https://www.entrepreneur.com/article/335195

NoiPA, Sogei rassicura: "Al momento non sono riscontrabili violazioni"

In relazione alle notizie che stanno girando in queste ore, di un probabile attacco informatico al sistema **NoiPA**, **Sogei** ha assicurato che sono in corso tutti gli esami del caso e che "***al momento***" **non sono riscontrabili violazioni** del sito in questione.

L’allarme scattato in mattinata è relativo a potenziali attività di ***phishing*** sulle utenze della piattaforma NoiPA, il sistema di gestione di stipendi e tredicesime per gli utenti della Pubblica Amministrazione, controllato dalla società in house del ministero dell’Economia e delle finanze.

Riguardo all’attacco, si legge sul sito stesso di NoiPA, “***sono stati rilevati limitati e circoscritti casi (15 su un totale di oltre due milioni di amministrati)*** *di modifiche dell’IBAN non confermati dal dipendente beneficiario. Tali casi sono stati prontamente gestiti, anche grazie all’intervento della Polizia Postale*”.

“*Al momento* – si legge sempre nella nota – *Sogei, la società in house del MEF che ha in conduzione il sistema NoiPA, sta analizzando e monitorando i dati al fine di garantire un puntuale presidio*”.
Per il momento **si raccomanda agli utenti “*di proteggere con la massima cura i dati di accesso al sistema NoiPA*,** *non comunicandoli a terzi, evitando di rispondere a email la cui provenienza o il cui mittente non siano riconosciuti e verificabili e che richiedano l’inserimento di dati sensibili*”.

In attesa di ulteriori indicazioni da Sogei e NoiPA, vale quanto spiegato sul sito della Polizia di Stato: “*Il phishing è catalogato come una particolare tipologia di truffa realizzata in rete attraverso l’inganno degli utenti. Si concretizza principalmente sfruttando messaggi di posta elettronica ingannevoli, come nel caso delle email apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l’accesso previa registrazione (web-mail, e-commerce ecc.)*“.
Il messaggio in questione, riferendo problemi di registrazione o di altra natura, “*invita a fornire i propri dati personali di accesso al servizio*“. Solitamente, nel messaggio, “*per rassicurare falsamente l’utente, è indicato un link che*

rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà, il sito a cui ci si collega è stato artificialmente allestito identico a quello originale, con lo scopo di sottrarre i dati sensibili al malcapitato utente".

Per saperne di più: Sogei

> *NoiPA, Sogei rassicura: "Al momento non sono riscontrabili violazioni"*

5G, Copasir: "Valutare di escludere Huawei e ZTE se a rischio la sicurezza nazionale"

Valutare l'ipotesi di escludere **Huawei** e **ZTE** dal **5G** in Italia, "*ove necessario per tutelare la sicurezza nazionale".* Questo il verdetto scritto dal Comitato parlamentare per la sicurezza della Repubblica (**Copasir**), presieduto dal **leghista Raffaele Volpi,** nella relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale (relatore: **Elio Vito** di **Forza Italia**).

"*Il Copasir non può che ritenere in gran parte fondate le preoccupazioni circa l'ingresso delle aziende cinesi nelle*

attività di installazione, configurazione e mantenimento delle infrastrutture delle reti 5G”, si legge nella relazione. “*Conseguentemente”,* è scritto nel documento dell’organo bicamerale, *“oltre a ritenere necessario un innalzamento degli standard di sicurezza idonei per accedere alla implementazione di tali infrastrutture”,* il Copasir *“rileva che si dovrebbe valutare anche l’ipotesi, ove necessario per tutelare la sicurezza nazionale, di escludere le predette aziende dalla attività di fornitura di tecnologia per le reti 5G”.*

Nella relazione si ricorda che “*lo sviluppo tecnologico in questo settore, che in una prima fase ha visto la prevalenza degli Stati Uniti, negli anni recenti ha fatto registrare una crescita rilevante delle aziende cinesi (**Huawei**, **ZTE**), che sono oggi protagoniste significative nell’ambito della tecnologia per la realizzazione delle reti 5G. Huawei in particolare ha notevolmente potenziato la sua presenza commerciale nel nostro Paese, ed oggi è uno degli attori fondamentali per la realizzazione della rete 5G. Contrariamente a quanto avviene per le imprese occidentali, le aziende cinesi, pur formalmente indipendenti dal potere governativo, sono tuttavia indirettamente collegate alle istituzioni del loro Paese, anche in virtù di alcune norme della legislazione interna”.*

“Non anteporre le esigenze commerciali e di mercato ai rischi sulla sicurezza nazionale”

“Appare certamente difficile, in una realtà caratterizzata dalle leggi del mercato e della libera concorrenza, prevedere interventi autoritativi che potrebbero mettere a rischio la stessa realizzabilità di progetti ritenuti essenziali per lo sviluppo delle nuove tecnologie”, continua la relazione ricordando il caso statunitense con l’entrata in vigore del divieto per Huawei rinviato più volte (da ultimo, l’entrata in

vigore del divieto è stata prorogata al febbraio 2020). *"Per queste medesime ragioni* – rileva il Copasir – *né gli organi della Ue, né i principali Paesi europei hanno finora adottato provvedimenti di divieto o limitazione alle attività degli operatori cinesi, pur nella consapevolezza dei possibili rischi che potrebbero derivarne".*

"*La rilevanza del problema è stata, peraltro, recentemente confermata in occasione del Consiglio dell'Unione europea Trasporti, telecomunicazioni ed energia del 3-4 dicembre 2019, che nelle conclusioni sul tema del 5G ha, tra l'altro, sottolineato come i Paesi membri debbano considerare fra i fattori di rischio per la sicurezza non solo i profili attinenti la tecnologia ma altresì quelli derivanti dalle politiche e dagli ordinamenti legislativi vigenti nei Paesi terzi dai quali vengono acquisiti prodotti e servizi" –* prosegue la relazione – *"In proposito, il Comitato ritiene di sottolineare che le pur significative esigenze commerciali e di mercato, che assumono un ruolo fondamentale in una economia aperta, non possono prevalere su quelle che attengono alla sicurezza nazionale, ove queste siano messe in pericolo".*

Mollicone (FdI): "Tutelare la sovranità digitale italiana"

"*Il documento conclusivo dei lavori dell'indagine sulla sicurezza delle telecomunicazioni del comitato parlamentare per la sicurezza della Repubblica conferma i nostri allarmi sulla presenza di aziende collegate con la Repubblica Popolare Cinese nelle nostre infrastrutture TLC. Il rischio viene dunque certificato dal Copasir, che prende in considerazione le normative di riferimento della Cina sulle aziende, che impone piena collaborazione e condivisione di informazioni con le gerarchie militari e politiche*". E' quanto ha dichiara il deputato responsabile Innovazione di Fratelli d'Italia, **Federico Mollicone**.

"Il combinato disposto della legge sulla Sicurezza Nazionale e quella sulla Sicurezza Cibernetica della dittatura comunista cinese obbliga", ha proseguito Mollicone, *"in via generale, cittadini e organizzazioni a fornire supporto e assistenza alle autorità di pubblica sicurezza militari e alle agenzie di intelligence ed impone agli operatori di rete di fornire supporto agli organi di polizia e alle agenzie di intelligence nella salvaguardia della sicurezza e degli interessi nazionali".*

"E' quindi necessario ora mettere in discussione la presenza di aziende cinesi come Huawei e ZTE nelle nostre infrastrutture strategiche, tutelando la sovranità digitale italiana", ha concluso il deputato, *"le informazioni e dati sensibili riconducibili a cittadini, enti e aziende italiani."*

Per saperne di più: 5G

> *5G, Copasir: "Valutare di escludere Huawei e ZTE se a rischio la sicurezza nazionale"*

Cyber sicurezza, domotica sotto attacco: "Danni per 4 sistemi smart home su 10"

Le imprese investono ancora troppo poco in sicurezza informatica. In termini di annunci tutti dichiarano di voler spendere di più a partire dal prossimo anno, ma nel frattempo il numero di attacchi è aumentato e con esso il volume

complessivo dei danni. In molti casi poi, le organizzazioni non hanno gli strumenti e le competenze per capire sino in fondo la natura di un attacco e per valutarne gli esiti.

Secondo una recente indagine Kaspersky, **il 55% delle aziende a livello internazionale è certo di non essere oggetto di attacchi informatici, mentre quasi un 39% però non è sicuro di conoscere a sufficienza le minacce potenziali che potrebbero riguardare la propria organizzazione**, di conseguenze non può neanche dire con precisione se è o no oggetto di attacchi.

D'altronde, le aziende, necessariamente sempre più connesse, costituiscono il bersaglio principale degli attacchi cyber, che hanno come obiettivo la sottrazione di dati a scopo di trarne un vantaggio economico. In occasione del convegno organizzato da Associazione IMQ, il Presidente **Maria Antonietta Portaluri** ha ricordato che "***gli attacchi cyber alle imprese sono aumentati di 10 volte nell'ultimo biennio*** *e sono in aumento*", aggiungendo, sì legge in una nota ANIE Confindustria, che "***nel primo semestre del 2019, hanno subito attacchi 4 computer su 10 impegnati nella gestione degli edifici dotati di sistemi digitali****. Tutto ciò ci deve portare ad aumentare gli investimenti in sicurezza*".

All'evento hanno partecipato, tra gli altri, anche **Giulio Iucci**, Presidente ANIE Sicurezza, **Stefano Mele**, Avvocato specializzato in Cyber Security, **Filippo Cavallarin**, Ricercatore ed esperto di sicurezza informatica, **Giacomo Stucchi**, Past President COPASIR – Consulente Regione Lombardia in tema di trasparenza, legalità e cyber security, **Guido Allegrezza**, Responsabile Compliance, Governance & Security di Telecom Italia Trust Technologies, **Stefano Zanero**, Professore Associato del Politecnico di Milano

Gli investimenti in sicurezza delle imprese italiane, inoltre, restano ancora molto bassi, secondo **Andrea Bianchi**, Direttore Area Politiche Industriali Confindustria: "***Il mercato della cyber security vale un miliardo di euro, pari soltanto allo 1%***

***della spesa high-tech aziendale**, quando un livello adeguato sarebbe intorno al 10% del totale*”.

Fondamentale, è dare valore all’industria di qualità, in grado di offrire già oggi al mercato soluzioni per garantire la sicurezza dei prodotti e sistemi, “*ed un valore certamente, avrà con sempre maggiore evidenza, la certificazione*”, ha ribadito Portaluri: “***Centralità del ruolo della certificazione** di fatto confermata dal Cybersecurity Act, Regolamento Europeo entrato in vigore a luglio per rafforzare il ruolo dell’Agenzia europea per la sicurezza e dare mandato per schemi di certificazione europei, a cui tutti dovremmo lavorare maggiormente*”.

Stando ai dati diffusi da una ricerca condotta da ServiceNow, nell’ultimo anno **gli attacchi informatici sono cresciuti del 17% in numero e, aspetto da non sottovalutare, del 27% come gravità**. Come ha ricordato un recente studio Acenture, i danni per le aziende potrebbero arrivare alla stratosferica cifra di 5.200 miliardi di dollari entro i prossimi cinque anni.

> *Cyber sicurezza, domotica sotto attacco: “Danni per 4 sistemi smart home su 10”*

Crittografia end-to-end, Facebook respinge le richieste di ‘backdoor’ di

William Barr

Facebook ha rifiutato la chiamata da parte dei governi di Stati Uniti, Regno Unito e Australia per creare una "backdoor" nelle sue app di messaggistica in modo che i funzionari delle forze dell'ordine possano accedere ai messaggi crittografati.

La società di **Mark Zuckerberg** tramite una lettera, ha respinto l'appello del Procuratore generale statunitense William Barr, mantenendo la sua decisione di rendere inaccessibili a terzi i messaggi scambiati sulle piattaforme di proprietà dell'azienda di Menlo Park.

Facebook Vs Barr

I ministri dei tre Paesi hanno pubblicato una lettera aperta lo scorso ottobre chiedendo a Facebook di interrompere i piani di estensione della crittografia end to end anche al suo servizio **Messenger**.

Ciò significherebbe che la polizia e altri funzionari delle forze dell'ordine non potranno accedere ai messaggi sulle piattaforme per indagare e perseguire i reati.

L'apertura delle piattaforme alle forze dell'ordine violerebbe il "*principio fondamentale*" della crittografia **end-to-end**, ha affermato Facebook, secondo cui **solo il mittente e il destinatario** di un messaggio hanno le chiavi per "sbloccare" e leggere ciò che viene inviato.

Nessun passo indietro per Facebook

"*Nessuno può intercettare e leggere questi messaggi – non noi, né i governi, né gli hacker o i criminali*", ha dichiarato

l’azienda in una lettera ai tre governi.

Inoltre, risulta impossibile interrompere la crittografia al solo scopo delle forze dell’ordine, senza indebolire la sicurezza in tutto il sistema, ha affermato Facebook.

“*I messaggi privati □□delle persone sarebbero meno sicuri e i veri vincitori sarebbero chiunque cerchi di trarre vantaggio da quella sicurezza indebolita. Non è qualcosa che siamo pronti a fare*“, ha comunicato l’azienda di Menlo Park.

Facebook ha affermato che continuerà a consultarsi con i gruppi dell’industria e della società civile sui modi per rafforzare la sicurezza sulle sue piattaforme e cooperare con le forze dell’ordine ove possibile “*purché sia □□coerente con la legge e non comprometta la sicurezza dei nostri utenti*“.

William Barr e la crittografia end-to-end

In un evento organizzato ieri dal **Wall Street Journal**, Barr è tornato alla carica sostenendo che applicazioni cifrate come WhatsApp e Signal hanno aiutato “*organizzazioni terroristiche, cartelli della droga, molestatori di bambini e bande dedite alla pedopornografia*“.

Le parole di Barr sono arrivate nello stesso giorno in cui Facebook e Apple sono state chiamate a testimoniare sulla crittografia davanti a una commissione del Senato Usa, in cui i dirigenti di Facebook e Apple hanno difeso le loro pratiche sulla privacy.

Il responsabile della privacy di Apple, **Erik Neuenschwander**, ha evidenziato l’importanza della crittografia su iPhone per proteggere dati sensibili come quelli bancari e sanitari e ha spiegato che non c’è modo di consentire l’accesso alle forze dell’ordine senza al contempo lasciare una porta aperta agli hacker.

https://www.key4biz.it/crittografia-end-to-end-facebook-respinge-le-richieste-di-backdoor-di-william-barr/282520/

Gli smartwatch per bambini venduti su Amazon sono facili da hackerare

I ricercatori di **Rapid7 Inc**., società di sicurezza informatica con sede a Boston, hanno scoperto delle vulnerabilità negli smartwatch per bambini venduti su Amazon.

Secondo la società, gli orologi intelligenti di fascia medio bassa, che vanno dai 20 a 35 dollari, hanno difetti critici che potrebbero consentire agli estranei di tracciare e parlare con chi li indossa.

Gli smartwatch testati da Rapid7 sono stati **Jsbaby Game Smart Watch** e Smartwatch per bambini **SmarTurtle**, tutti realizzati dalla società cinese **3G Electronics.** Rapid7 ha testato solo tre dell'ampia varietà di smartwatch per bambini economici venduti su Amazon, quindi è possibile che altri modelli contengano gli stessi difetti.

"*È possibile che un utente malintenzionato con conoscenza del numero di telefono dello smartwatch possa assumere il controllo totale del dispositivo e quindi utilizzare la funzionalità di tracciamento e chat vocale con le stesse autorizzazioni dell'utente legittimo (in genere un genitore)*", ha dichiarato a **Bloomberg Tod Beardsley**, direttore della

ricerca di Rapid7.

Le problematiche degli smartwatch

Questi smartwatch sono dotati di funzioni GPS e di chat vocale, e i loro prezzi bassi, le funzionalità limitate e la facilità d'uso rispetto agli smartphone li rendono molto popolari per i genitori che vogliono sapere dove si trovano i loro figli o comunicare con loro senza smartphone.

Nonostante ciò Rapid7 ha affermato che questa misura di sicurezza, una whitelist, era un "controllo debole, anche nelle migliori circostanze".

Un modo in cui un tutore può modificare le impostazioni dello smartwatch di un bambino da remoto è l'invio di un messaggio di testo al dispositivo. Ma per impedire agli estranei di modificare le impostazioni, è possibile creare un elenco di determinati numeri pre-approvati. Ma Rapid7 ha affermato che questa misura di sicurezza, una whitelist, era un "*controllo debole, anche nelle migliori circostanze*".

La società di Boston ha scoperto che la whitelist non aveva alcun effetto su chi potesse modificare le impostazioni dello smartwatch. Chiunque, anche quelli che non erano nell'elenco pre-approvato, potrebbe inviare un messaggio di testo a uno di questi smartwatch per modificare le proprie impostazioni.

"*In pratica, questo filtro non sembrava affatto funzionale*", ha dichiarato Beardsley.

L'altro difetto include le password predefinite dello smartwatch "12345" impostata per tutti i dispositivi. Rapid7 ha scoperto che i manuali dello smartwatch avevano poche o nessuna informazione sulle password predefinite e su come modificarle. A causa di questo ostacolo, è improbabile che gli utenti cambino la password predefinita, il che rende facile a chiunque l'accesso agli smartphone per ottenerne il controllo

Impossibile rintracciare i produttori

Questo problema di sicurezza potrebbe essere risolto con un aggiornamento del firmware adottato dal fornitore, ma "*è improbabile che un tale aggiornamento si materializzi dato che i fornitori di questi dispositivi sono difficili o impossibili da individuare*", ha aggiunto la società di sicurezza informatica.

Rapid7 ha dichiarato che i suoi ricercatori non sono stati in grado di contattare nè i venditori né quello che credono sia il produttore degli orologi intelligenti, una società cinese chiamata **3g Electronics Co.**

Il consiglio di Rapid7 è di attenersi solamente a "*venditori chiaramente identificabili*". In sostanza, se riconoscete questo marchio, statene alla larga.

https://www.key4biz.it/gli-smartwatch-per-bambini-venduti-su-amazon-sono-facili-da-hackerare/282462/

Violato il Cloud di Google: i dati di 1,2 miliardi di persone trovati su un server non protetto

Un database conservato sul **Cloud di Google** contenete i dati esposti senza protezione di 1,2 miliardi di persone sono stati rinvenuti in quello che già viene definito come un colossale

data leak. Fra i dati esposti in rete c'erano account social, indirizzi mail e numeri di telefono associati ai nominati. Il data breach è stato scoperto il mese scorso dall'FBI e ad oggi non è chiaro come la gran massa di dati, pari a 4 terabyte, sia finita online. Numeri di telefono, indirizzi mail, profili Facebook, Twitter, LinkedIn oltre a nome e cognome. Il server incriminato è stato chiuso e per ora nemmeno l'FBI commenta l'accaduto.

Mega leak scoperto da un esperto negli Usa

Il mega leak, scoperto da un ricercatore americano specializzato in security, si chiama **Vinny Troia** ed è il Ceo della società **Night Lion Security** con sede a St. Louis, è stato subito denunciato all'FBI e ne ha dato notizia per la prima volta a ottobre da *Wired* e ripreso poi qualche giorno fa dall'agenzia *Bloomberg*, secondo cui la maggior parte dei dati è stata raccolta su un server Google Cloud da una società chiamata **People Data Labs**, che gestisce i dati di un miliardo e mezzo di persone di cui 260 milioni negli Usa, ma che nega che sia il suo server ad aver subito il leak.

Tutti i numeri del leak

Secondo quanto riferito da *Appleinsider.com*, i dati esposti rinvenuti sul server non contenevano dettagli sensibili, come estremi di pagamento o password, ma diverse informazioni di base tratte possibilmente dai social media. Fra questi dati il nome, il numero di cellulare, i link ai profili social. Complessivamente 50 milioni di numeri di cellulare unici sono stati rinvenuti e 622 milioni di indirizzi mail.

Ad ogni buon conto, secondo il sito specializzato *Data Viper*, la società People Data Labs gestisce:

- I dati di più di 1,5 miliardi di persone, di cui 260 milioni negli Usa.
- Più di un miliardo di indirizzi email. L'email di lavoro di più del 70% dei decision maker negli Usa, UK e in Canada.
- Più di 420 milioni di url di Linkedin.
- Più di 1 miliardo di url e personal id di Facebook.
- Più di 400 milioni di numeri di telefono. Più di 200 milioni di numeri di cellulare negli Usa.

I dati non protetti non si trovavano su un server della People Data Labs, ma piuttosto su un server di **Google Cloud**, ha dichiarato Troia. Il server è stato chiuso dopo il ritrovamento.

No comment di Google alla domanda su chi aveva affittato il server.

"E' la prima volta che vedo email, nomi e numeri e profili connessi a Facebook, Twitter, LinkedIn e Github tutti in un unico posto", ha detto Troia, che si autodefinisce come un cacciatore di cybercrime. *"Non ci sono password connesse a questi dati, ma avere a disposizione grandi set di password non è più così eccitante".*

Dati provenienti da diverse fonti?

Sean Thorne, cofondatore e Ceo di People Data Labs, ha detto che gran parte dei dati, ma non tutti, provengono dalla sua società e sospetta che siano stati aggregati da un'altra azienda che li avrebbe raggruppati da diverse fonti.

"Noi prendiamo l'impegno che i nostri dati raccolti all'ingrosso (bulk data) non siano esposti", scrive sul suo sito People data Labs, precisando che il tema della pirvacy è

alquanto sentito in azienda e che diversi professionisti si occupano di scoprire e proteggere data set di dati vulnerabili online prima che finiscano sul mercato nero.

Troia, che ha fatto la scoperta del mega leak a ottobre durante un controllo di routine, ha subito denunciato il ritrovamento di 4 terabyte di dati incustoditi e la loro location all'FBI. Il server incriminato è stato chiuso e per ora nemmeno l'FBI commenta l'accaduto.

Troia ha poi aggiunto di non avere idea di chi abbia lasciato i dati sul server, chiamando in causa non meglio precisati hacker malintenzionati o possibilmente i clienti stessi di People Data Labs. Di fatto, particolarmente preziosi nelle mani di criminali hacker o rivenditori e fabbricanti di fake news sarebbero gli account dei social media.

https://www.key4biz.it/violato-il-cloud-di-google-i-dati-di-12-miliardi-di-persone-trovati-su-un-server-non-protetto/280608/

Conte rilancia la priorità della cyber sicurezza, ma al Paese manca un cloud nazionale per i dati della PA

Il Presidente del Consiglio, **Giuseppe Conte**, intervenendo a Milano alla prima tappa di "***Asset – L'intellig&nce per le Imprese***" del Dipartimento delle informazioni per la sicurezza (Dis), ha rilanciato sul tavolo un tema forte, fondamentale quanto poco dibattuto a livello pubblico: la sicurezza nazionale, "*il più immateriale, il meno visibile ad occhio*

nudo tra i beni collettivi, al tempo stesso il primo di essi".

Ne ha parlato in termini di sicurezza delle organizzazioni, dell'industria e delle imprese, della Pubblica Amministrazione e delle infrastrutture strategiche, ma soprattutto in termini digitali e di ***cybersecurity***. Di difesa informatica del nostro patrimonio industriale, scientifico e tecnologico.
Oltre alle grandi realtà industriali e al mondo imprenditoriale italiano, "*anche la Pubblica Amministrazione ha deciso di porsi alla testa del processo di modernizzazione tecnologica del Paese*", ha dichiarato Conte.

"*Il valore strategico della trasformazione digitale cresce a dismisura ed in maniera trasversale a tutti i comparti produttivi, al punto che i cosiddetti "**digital enablers**" sono divenuti un volano decisivo per lo sviluppo e la competitività di qualsiasi economia*", ha evidenziato il Presidente del Consiglio nel suo intervento. "*Tuttavia, la necessità imprescindibile di cavalcare l'innovazione dovrà andare di pari passo con la cura, non meno essenziale, nel mitigare le crescenti vulnerabilità insite nelle basse barriere all'ingresso che contraddistinguono lo spazio cibernetico*".

Va da sé, che con l'avvento del **5G** e dell'**internet delle cose** "*l'intero comparto aziendale italiano rischierebbe di finire ai margini della competizione internazionale se non ponesse la sicurezza al vertice delle proprie priorità, così come è cognizione diffusa che i condizionamenti ed i guasti causati dalle minacce cibernetiche si ripercuotono negativamente su tutta l'economia nazionale*".
"*Serve quindi un cambiamento di paradigma culturale, che metta al centro la prevenzione, perché **la cybersecurity non deve essere più percepita come un semplice costo, bensì come un investimento***", ha precisato il Premier.

Un discorso che arriva un po' tardi nel nostro Paese, ma che ha il merito di rilanciare, una volta di più, il tema della cyber sicurezza. Un tema centrale per le imprese e le industrie, certamente, ma che sembra considerare poco, pochissimo o per niente, addirittura, l'**altro argomento altrettanto strategico** e non più rimandabile: la **tutela dei dati sensibili**.
Sempre più spesso le amministrazioni pubbliche centrali e locali neanche trattano più con le grandi corporation tecnologiche, perchè le cosiddette ***big tech*** o *Over the top* (OTT), tra cui le più potenti al mondo sono **Amazon**, **Microsoft**, **Google**, **Facebook** ed **Apple**, entrano direttamente e con facilità nelle stanze delle Istituzioni.

Negli Stati Uniti, **una grossa fetta degli investimenti lobbistici effettuati dagli OTT (circa 582 milioni di dollari, sarebbe stata indirizzata proprio nel convincere politici ed opinione pubblica nella "bontà" di affidare con fiducia alle aziende più grosse i nostri dati**: non solo quelli anagrafici, ma ogni singolo byte relativo alla nostra geolocalizzazione, alla nostra routine quotidiana, ai nostri gusti musicali o gastronomici e perché no politici. Una miniera a cielo aperto per chi controlla gli strumenti utili a farne business. A quanto pare però, la questione sta diventando spinosa: tolto il coperchio, sotto ribolle la necessità di adeguare anche negli Usa la gestione e conservazione dei dati a una regolamentazione dinamica e capace di limitare gli abusi.

Il Presidente del Consiglio sembra non considerare come "*problema*" questo rapporto privilegiato della Pubblica Amministrazione (la PA, quindi lo Stato) con le multinazionali dell'economia digitale, un rapporto ambiguo e poco trasparente, dove al centro della trattativa ci sono sempre i dati.
Gli OTT o giganti del web assicurano che la loro politica è finalizzata ad assicurare e garantire la piena sicurezza dei dati della PA, quando **il vero problema sta proprio**

nell'affidare a queste realtà "*esterne*" i nostri dati. Dati che andrebbero affidati a società della Pubblica Amministrazione, se non fosse che **al Paese manca una società pubblica di cloud, manca un cloud nazionale**.

Un argomento scottante, di cui abbiamo parlato nei giorni scorsi con l'**accordo annunciato tra TIM e Google**, proprio per l'offerta congiunta di servizi cloud e che porta con sé criticità serie sui potenziali risvolti in tema di protezione dati.
Questo accordo riguarderà anche i dati della Pubblica Amministrazione?
I dati degli italiani conservati nei data center di Tim andranno in mano a Google?
Sono tante le domande da porsi, perchè alta deve rimanere l'attenzione su un'argomento è a dir poco delicato, sia per i cittadini, sia in termini di sicurezza nazionale.

Senza dimenticare il caso "*Piacentini*" in Italia di qualche anno fa, con la nomina dell'allora Senior Vice Presidente di Amazon a Commissario straordinario del governo per il digitale e l'innovazione da parte del Governo Renzi, che aprì di fatto un confronto sulla proprietà dei dati, la loro conservazione e gestione anche nel nostro Paese.

Dati che sono il carburante della crescita economica, ma che proprio per questo dovrebbero essere considerati "*risorsa strategica*", da tutelare, gestire con cura, proteggere. Dati non solo relativi ai cittadini (e nel caso della PA anche di questo parliamo), ma anche alle imprese, le industrie, le infrastrutture, che giustamente stanno al centro dell'azione di Governo.

La politica dovrebbe occuparsi maggiormente di questo argomento così importante, come già sta accadendo in Francia e Germania peraltro, perchè il nostro Paese corre il rischio serissimo di consegnare i dati dei suoi cittadini e delle sue organizzazioni economico-industriali nelle mani di poche

corportation, che ne faranno strumento privato di profitto e vantaggio.

> *Conte rilancia la priorità della cyber sicurezza, ma al Paese manca un cloud nazionale per i dati della PA*

5G e cybersecurity, tra attacchi DDoS e Botnet cosa c’è in agguato?

La crescita e lo sviluppo delle nuove reti **5G** è sicuramente un argomento caldo, ma come con l’avvento di qualsiasi nuova tecnologia si sono sollevati alcuni dubbi sulla sua introduzione – e non solo di carattere strutturale –, dubbi ribaditi anche in un recente report dell’Unione Europea.

A differenza delle precedenti connessioni come 3G e 4G il network loro erede sarà – per la maggior parte – basato su software e virtualizzato.

L’avvento del 5G

Questo rappresenta una grossa frattura rispetto al passato, dove i network erano storicamente confinati e limitati dall’hardware a loro disposizione, trasformando le funzioni del network tradizionale in funzioni virtuali, il tutto orchestrato attraverso un software di controllo.

Sempre parte del pacchetto di novità introdotto con il 5G sarà l’uso massiccio della tecnologia di ***Edge Computing*** dove le

applicazioni, l'attività di archiviazione e tutte le funzioni di controllo saranno obbligate ad operare relativamente vicine agli end user e ai vari endpoint IoT.

Questo è un *paradigm shift* non indifferente, dall'architettura centralizzata del network 4G stiamo passando a un'architettura diffusa e – in maniera più preoccupante – creando un perimetro d'attacco decisamente più ampio per i Criminal Hacker.

Stiamo correndo il rischio di esporre i network mobile a insidie mai riscontrate prima. Il report pubblicato dall'Unione Europea ha messo in guardia sui vari rischi legati ai fornitori e alla fase di sviluppo software, in particolare per quanto riguarda la catena dei fornitori.

Il rischio di delegare troppo all'IoT

L'inevitabile proliferazione dei software per sostenere e portare avanti l'infrastruttura 5G è, come anticipato una delle maggiori preoccupazioni dell'UE.

Il problema infatti non è insisto nella sicurezza della tecnologia 5G in sé e per sé, nonostante alcuni esempi pratici della sua possibile vulnerabilità di questa tecnologia – come la possibilità per possibili attaccanti di utilizzare ripetitori "falsi" virtuali per dirottare il traffico e sottrarre informazioni -. In generale, infatti, il 5G può vantare una maggiore capacità di crittografare i dati e un superiore algoritmo di verifica della legittimità degli utenti connessi rispetto al suo antenato.

Ma il vero punto debole dal punto di vista della Cybersecurity del 5G è sicuramente il traffico di dati tra i tantissimi *endpoint* ***IoT*** connessi a Internet grazie a questa tecnologia.

Stiamo parlando di una mole e di una varietà di device – che spaziano dalle auto ai robot industriali fino ai semplici oggetti di domotica – impressionante e soprattutto che opera secondo una moltitudine di standard di sicurezza fin troppo variegata. Secondo le stime più conservative di Gartner questi arriveranno ad essere circa 25 miliardi entro la fine del prossimo anno.

Tutti questi, naturalmente, passeranno a breve sulle nuove reti 5G fornendo di fatto ai Criminal hacker una superfice d'attacco senza precedenti. Non è una novità d'altronde che non ci sia bersaglio più ambito da questi gruppi delle new entry nel mondo della tecnologia, sia perché tra i Criminal Hacker vige una certa competizione sia perché le nuove tecnologie sono sempre le più vulnerabili.

C'è anche un'altra grande questione legata alla provenienza e all'affidabilità dei vari produttori dei device IoT – non che i grandi nomi del settore tech siano immuni a questi "scivoloni" – provenienti in particolar modo dal sud-est asiatico. Affidereste la sicurezza dei vostri dati a uno dei più disparati mobile che si possono acquistare su siti di e-commerce come Aliexpress?

5G: il rischio DDoS e Botnet

I Criminal Hacker possiedono già l'abilità di scannerizzare centinaia di migliaia di device in cerca di possibili falle – anche le più banali come quelle legate alle password di default che non vengono cambiate al momento della messa in commercio del prodotto (da "admin" a "guest").

Non è solo una previsione di catastrofismo tecnologico; non è passato molto tempo dall'attacco "**Mirai Botnet**" del 2016 che aveva sfruttato debolezze di questo genere trovate in migliaia di device "connessi" come fotocamere, router e videocamere per prenderne il controllo e "abbattere" siti come **Twitter, il New York Times e Spotify.**

I criminali, nel dettaglio, avevano utilizzato un “merge” di due tecniche differenti, ma comunque conosciute: prima un botnet – che appunto prende il controllo dei dispositivi IoT e li utilizza per sferrare un Cyber attacco – e successivamente un DDoS, in grado di sovraccaricare il network bersaglio con un numero eccessivo di richieste.

Cosa c’è in agguato?

Il rischio, in futuro, potrebbe essere che quando i Criminal Hacker riescono a violare un dispositivo collegato al 5G, la velocità della rete permetterà loro di estrarre e scaricare informazioni, compresi i dati personali e le informazioni sui clienti, molto più velocemente di prima.

La probabilità di trovare un dispositivo IoT che non è stato settato propriamente, o con una password debole, come accennato, è al momento piuttosto alto. Come se non bastasse, poiché i dispositivi IoT si collegano direttamente alla rete mobile, i Criminal Hacker non dovranno aggirare il framework di sicurezza – tradizionalmente più resiliente – delle reti domestiche o aziendali. C’è anche il rischio che le case che utilizzano dispositivi di domotica 5G diventino più vulnerabili.

Se il software di sicurezza di frigoriferi, allarmi anti-fumo e altri dispositivi “intelligenti” connessi a Internet non viene aggiornato regolarmente, una singola falla potrebbe esporre un’enorme quantità di dati. Anche le aziende dovranno necessariamente mettersi in guardia dai potenziali rischi nel caso in cui i dipendenti utilizzano reti 5G piuttosto che le loro reti aziendali per inviare dati riservati.

Ci sono anche alcuni problemi “*legacy*” che si trascinano dal tempo della prima implementazione del 3G. La nuova tecnologia utilizza ancora la **Authentication and Key Agreement (AKA) u**n sistema virtuale che permette ai vari network di identificarsi correttamente.

3 macro aree di criticità

Nel 5G questo sistema ha due criticità ancora latenti: permette a un Threat actor di spostare la propria fattura e il conto del consumo di traffico su un altro ignaro utente e – in maniera più preoccupante – permette il tracking dei dispositivi vicini.

C'è anche un fattore stressogeno più umano: l'effort necessario in termini di costo e ore di lavoro per implementare la nuova soluzione rispetto al 4G che alcuni team IT incaricati potrebbero essere più proni ad errori in fase di rollout, causando falle e problematiche di sicurezza non volute.

Riassumendo possiamo dire che ci sono tre macroaree di criticità legate all'introduzione del 5G che potrebbero introdurre una nuova dimensione di Cyber risk:

- L'insieme delle tecnologie che danno vita al 5G non è ancora sufficientemente testato;
- Permette accesso e movimento di una quantità enormemente più grande di dati e di conseguenza amplia la superfice d'attacco
- È una scommessa, molto più del 4G verrà utilizzato come base per applicazioni "mission-critical" (d'importanza centrale per il funzionamento di un dato servizio).

Sembra una strada senza uscita, ma in realtà quello che deve accompagnare l'implementazione del 5G e una maggiore e rinnovata attenzione agli standard di sicurezza adottati dai produttori che devono essere necessariamente rinforzati e condivisi.

"Yoda: Vittoria? Vittoria, tu la chiami, maestro Obi-Wan? No, non vittoria. Su tutto l'ombra del lato oscuro è calata. Cominciata la Guerra dei Cloni è." (Star War)

Le novità sono sempre eccitanti, ma forse con il 5G dobbiamo

adottare un approccio più cauto e misurato.

https://www.key4biz.it/5g-e-cybersecurity-tra-attacchi-ddos-e-botnet-cosa-ce-in-agguato/279892/