Fastweb investe in sicurezza e rileva il 70% di 7Layers

Fastweb prosegue nella strategia di costante rafforzamento dell'offerta di Cybersecurity e acquisisce il 70% di **7Layers**, società leader nei servizi per la sicurezza informatica, fondata nel 2012 a Firenze e inserita per quattro anni consecutivi, dal 2017 al 2020, dal *Financial Times* nella classifica delle 1.000 "fastest-growing companies" a livello europeo.

Modello OTT infrastrutturato

Lo scrive l'azienda in una nota, aggiungendo che in linea con la recente acquisizione nel perimetro aziendale di **Cutaway**, società specializzata in servizi Cloud, anche l'operazione conclusa con 7Layers si inserisce nel più ampio percorso di posizionamento sul mercato di Fastweb come OTT Infrastrutturato, anche nell'ambito della Cyber Security, una componente sempre più rilevante per il settore Enterprise. Un percorso che oltre alla crescita per linee esterne è sostenuto dai contestuali e significativi investimenti in tecnologia e infrastrutture, che nel solo primo semestre 2020 hanno raggiunto i 276 milioni di Euro.

L'integrazione

L'integrazione delle soluzioni di 7Layers nell'offerta Fastweb consentiranno alla clientela Enterprise di beneficiare di servizi aggiuntivi coprendo integralmente il proprio fabbisogno di protezione e di sicurezza contro le minacce informatiche. Alla già solida proposta di Fastweb di servizi

principalmente legati alla protezione delle infrastrutture di rete monitorate costantemente dal Security Operation Center (SOC), si aggiungono quindi soluzioni avanzate di Threat Management e di Threat Intelligence, l'area della Security più innovativa e in forte crescita, di cui 7Layers è leader, che permette di aumentare sensibilmente il livello di protezione dell'IT aziendale grazie ad un approccio preventivo e alla capacità di gestione e di mitigazione degli attacchi più evoluti (Managed Detection and Response).

Mondo business

L'integrazione dei servizi e la collaborazione con i professionisti altamente specializzati di 7Layers consentirà dunque a Fastweb non solo di rispondere a tutte le esigenze di protezione dei propri clienti con un portafoglio strutturato e completo di servizi di Cyber Security ma anche di avere il controllo diretto end-to-end dell'intero ciclo di vita dei servizi erogati e di rispondere ancora più velocemente alle esigenze del mondo business.

"Dopo l'operazione Cutaway nell'ottica di una rapida crescita nei servizi Cloud, con questa nuova operazione puntiamo a rafforzare il nostro posizionamento come Security Provider per il mondo delle aziende" ha dichiarato **Alberto Calcagno**, Amministratore Delegato di Fastweb. *"L'expertise di 7Layers unita alla nostra profonda conoscenza delle tecnologie di rete genereranno sinergie estremamente interessanti confluendo in un patrimonio che Fastweb metterà a frutto per crescere rapidamente in questo settore chiave rispondendo alla sempre più forte e distribuita necessità di sicurezza delle imprese".*

"Con questo accordo potremo estendere la nostra proposizione di soluzioni Cybersecurity innovative e flessibili rispondendo alle esigenze di un mercato sempre più veloce e integrato", hanno commentato **Fabrizio Rosina** e **Riccardo Baldanzi**,

Amministratori Delegati di 7Layers. *“Le minacce informatiche crescono ogni giorno, così come aumenta costantemente la presenza del mondo digitale nelle nostre vite. Insieme a Fastweb, che da sempre punta all’innovazione e un rapporto diretto sul territorio, sarà possibile estendere le soluzioni di sicurezza a tutti i mercati”.*

https://www.key4biz.it/fastweb-investe-in-sicurezza-e-rileva-il-70-di-7layers/323716/

Ue, al via il CyberSecurityMonth. Vestager: “La cybersecurity riguarda tutti noi”

“Prima di cliccare, pensaci”. E’ questo il claim dell’ottava edizione del mese europeo della cybersecurity, che riunisce l’Unione europea, i suoi Stati membri e i cittadini europei per prevenire e contrastare le minacce informatiche.

L’obiettivo principale della campagna di quest’anno, che inizia oggi, 1º ottobre, è garantire che i cittadini siano consapevoli dei rischi online e dispongano degli strumenti necessari per diventare utenti di tecnologie più resilienti e più sicuri.

“Visto che la nostra vita quotidiana e le nostre economie stanno diventando sempre più dipendenti dalle soluzioni

digitali, dobbiamo renderci conto che la sicurezza informatica riguarda tutti noi”, ha dichiarato **Margrethe Vestager**, Vicepresidente della Commissione Europea titolare per la Concorrenza. *“È importante promuovere una cultura della sicurezza all’avanguardia nei settori vitali della nostra economia e della nostra società.”*

Margaritis Schinas, Vicepresidente responsabile per la Promozione dello stile di vita europeo, ha aggiunto:*”Il mese europeo della cybersecurity mira a sensibilizzare l’opinione pubblica sulla sicurezza informatica e a renderci consapevoli delle minacce informatiche. Ci rammenta che possiamo facilmente rafforzare la nostra cibersicurezza adottando buone abitudini digitali. E’ essenziale per il nostro stile di vita europeo.”*

Thierry Breton, Commissario per il Mercato interno, ha concluso: *“Come lo spazio terrestre, marittimo o aereo, lo spazio dell’informazione digitale presenta talvolta lacune in materia di sicurezza, lacune che vanno colmate. La nostra ambizione è fornire ai cittadini dell’UE lo spazio dell’informazione più sicuro al mondo. A tal scopo ci affideremo soprattutto all’istruzione. È questo l’obiettivo del mese europeo della cybersecurity 2020, che lanceremo domani per sensibilizzare i cittadini sulle competenze in materia di sicurezza online e cibersicurezza, fondamentali per il futuro.”*

Ottobre mese europeo della Cybersecurity

Per l’intero mese in tutta Europa si svolgeranno centinaia di attività, coordinate dall’Agenzia europea per la cibersicurezza (ENISA).

Si terranno conferenze, seminari, sessioni di formazione, presentazioni generali, webinar e campagne online, mirate a

sensibilizzare i cittadini sulla cybersecurity ed a fornire informazioni aggiornate sulla sicurezza digitale attraverso la formazione e la condivisione delle migliori pratiche.

L’Italia e la sicurezza informatica

Nelle ultime settimane in Italia si è visto un incremento massiccio di attacchi informatici rivoli ad Istituzioni ed imprese. Il più grave, per le conseguenze avute, rimane l’attacco al **Gruppo Carraro**, azienda italiana leader internazionale nel comparto delle macchine agricole.

L’azienda, a causa dell’attacco subito che ha paralizzato i sistemi informatici di tutta l’attività del gruppo, da quella amministrativa a quella produttiva, altamente automatizzata da robot, ha dovuto mettere settecento dipendenti in cassa integrazione tra gli stabilimenti di Campodarsego e quelli della divisione Agritalia di Rovigo in attesa del ripristino dei sistemi.

L’attacco informatico era avvenuto a distanza di pochi giorni da quello analogo che aveva colpito **Luxottica**, la più grande produttrice mondiale di montature per occhiali da vista e da sole

https://www.key4biz.it/ottobre-e-il-mese-europeo-della-cybersecurity-vestager-la-sicurezza-informatica-riguarda-tutti-noi/323683/

Alien, il banking trojan

prende di mira social network e app

La società di sicurezza informatica ThreatFabric ha diramato con il suo ultimo rapporto un’alert riguardo a una nuova cyber minaccia che sta prendendo di mira non solo le app bancarie ma anche social network, servizi di messaggistica istantanea e di posta elettronica di diversi Paesi tra cui Italia, Germania, Francia, Regno Unito, Stati Uniti e Australia.

Si chiama Alien, ed è un trojan in grado di carpire dati da centinaia di app.

Il malware “Alieno”

Secondo gli esperti di sicurezza, Alien rilasciato a inizio anno come Malware-as-a-Service nei forum underground, condividerebbe parte del codice sorgente di Cerberus, il noto malware che, dopo aver avuto il maggior successo nei mesi di giugno e di luglio 2020, ad agosto alcuni bug per lungo tempo lasciati irrisolti ne hanno decretato il declino consentendo, nel frattempo, al team Google Play Protect di trovare dei metodi di rilevamento e rimozione.

Le contromisure rivelatesi efficaci per Cerberus tuttavia non sembrano avere effetto contro Alien che s’impone come un trojan bancario mutevole e adattativo di tutto rispetto, tanto da essere definito “Alieno”.

Tra le capacità confermate di questo malware figurano quelle di poter accedere facilmente alla lista dei contatti, carpire messaggi SMS, installare/rimuovere applicazioni e monitorare in generale tutte le attività del dispositivo infetto. Alien è

in grado anche di creare con tecniche overlay numerose false interfacce app, nonché di intercettare i codici generati per l'autenticazione a due fattori (2FA).

Pur basandosi sullo stesso codice di Cerberus e condividendo buona parte delle funzionalità, i ricercatori affermano che gli sviluppatori di Alien hanno personalizzato il protocollo di comunicazione C2 e aggiunto due ulteriori componenti, non presenti in nessuna delle versioni di Cerberus, ovvero un controllo remoto basato su TeamViewer (componente RAT) e uno sniffer per le notifiche (componente stealer).

Alien – la componente RAT

La componente RAT (Remote Access Trojan) implementa un set di comandi dedicati e diversi da quelli previsti dal gestore C2 dei comandi principale.

TeamViewer una volta installato non viene subito attivato. Il Trojan attende la ricezione delle credenziali per configurare la connessione al server TeamViewer e utilizza i privilegi di accessibilità per accedere all'applicazione stessa concedendo eventuali altre autorizzazioni aggiuntive. Solo dopo questa fase d'inizializzazione, se TeamViewer supporta il dispositivo target, gli attaccanti possono ottenere il controllo remoto completo dell'interfaccia utente del dispositivo, monitorando in tempo reale anche il comportamento dell'utente. In caso contrario TeamViewer funzionerà solo in modalità streaming video.

Alien – la componente Stealer

La componente stealer abusa dell'autorizzazione "*android.permission.BIND_NOTIFICATION_LISTENER*_SERVICE" per ottenere il contenuto delle notifiche della barra di stato sul dispositivo infetto. Sebbene questa autorizzazione deve essere concessa dall'utente manualmente, il malware utilizzando i

privilegi di accessibilità è in grado di eseguire in autonomia le interazioni necessarie allo scopo. In tal modo dopo aver ottenuto tali autorizzazioni, tutte le notifiche vengono inviate al server di comando e controllo C2.

Conclusioni

L'aver rilasciato gratuitamente sui forum di hacking il codice sorgente del trojan Cerberus v2 (notizia annunciata di recente da Kaspersky Lab), ha certamente dato adito agli sviluppatori malevoli concorrenti di generare nuove famiglie di malware derivate. È, infatti, ragionevole pensare che bisognerà attendersi un'evoluzione di tale evenienza.

Anche il trend in costante crescita dell'interesse dei criminal hacker a voler capitalizzare le informazioni che si riescono a carpire soprattutto dai dispositivi mobili, divenuti oramai una preziosa fucina informativa, non fa di certo ben sperare.

Nell'appendice dell'articolo pubblicato da ThreatFabric vengono riportati gli elenchi dei campioni trovati in natura (12) e dei package compromessi (226). https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html

Alien, il banking trojan prende di mira social network e app

A Business Leader's Beginner

Guide to Cybersecurity

Take advantage of available cybersecurity solutions to protect your business and its digital assets.

September 26, 2020 4 min read

Opinions expressed by *Entrepreneur* contributors are their own.

According to Statista, there are about 4.57 billion active internet users globally as of July 2020. This number is great for businesses, especially those that are powered by the digital economy.

As businesses continue to embrace the tech age as well as the opportunities that come with it, the presence of cybercriminals is increasing, too. The activities of these criminals cannot be ignored, as they are capable of crashing any business. Business leaders who wish to remain in business must pay better attention to cybersecurity.

Related: The Real Cost of a Data Breach for Your Brand (and How to Best Protect Yourself)

Whilst there is no definitive solution to what is seen as the biggest threat to modern businesses — cybercrime — business owners like you can take advantage of available cybersecurity solutions and knowledge to protect your business and its digital assets. Below are three things to help you get started:

1. Get everyone involved

The days when cybersecurity was seen as just the job for the IT team are over. Business leaders all over the world are

realizing this and you need to do the same.

In a Harvard Business Review, cybersecurity experts Thomas J. Parenty and Jack J. Domet insist that no amount of technology, resources, or policies will reverse the trend that has seen cybercrimes rise. *"Only sound governance, originating with the board, can turn the tide. Protection against cyberattacks can't be treated as a problem solely belonging to an IT or cybersecurity department. It needs to cast a wide and impenetrable net that covers everything an organization does—from its business operations, models, and strategies to its products and intellectual property."*

Related: Why IT Security Will be a Prime Concern for Businesses in the Next Decade

A cyberattack can occur when an innocent employee clicks a malicious link from a device belonging to the business. The drill has to affect the least person associated with the business. There is a real threat out there, your business and her assets are at stake. Everyone in your business needs to understand this as much as you do.

2. Develop a policy on cybersecurity

Preaching about the importance of cybersecurity alone may not get the job done, a policy that spells out your business' protocols with regards to cybersecurity is necessary. A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media.

Non-IT employees are usually the weakest links in cybersecurity efforts. These employees typically share passwords, click on links, download attachments, with little knowledge about encrypting data. All of these open the door to

cyberattacks and can comprise the security of your business.

Setting up a policy on cybersecurity would help your employees and third parties with access to your digital assets understand how to keep your data secured and safe from the prying eyes of cybercriminals. You must take responsibility for creating a culture that prioritizes security; this would enhance the credibility status of your business.

Related: Why Small Businesses Must Deal With Emerging Cybersecurity Threats

According to FCC, adhering to the following tips would help to ensure the security of your business and her digital assets:

1. Protect information, computers, and networks from cyber attacks
2. Create a mobile device action plan
3. Make backup copies of essential business data and information.
4. Control physical access to your computers and create user accounts for each employee
5. Secure your Wi-Fi networks
6. Employ best practices on payment cards
7. Limit employee access to data and information, limit authority to install software
8. Passwords and authentication

Setting up a policy on cybersecurity for your business might seem like another tedious task or process to execute, but the benefits outweigh the cost: do it now!

3. Get a trusted Virtual Private Network (VPN)

The risks of going online are enormous. The reality is this: if you are not online then cybercriminals stand no chance with you. A Virtual Private Network (VPN) is a tool that allows you to interact with the internet anonymously, thereby drastically reducing your exposure to cybercrimes.

With leading VPN providers like Express VPN, Nord VPN, and Switcherry offering unlimited speed, unlimited Bandwith, and free servers in the US help individuals and businesses tackle the prevalent cyber threats and keep their digital assets free from prying eyes by providing a secure connection from all types of tracking.

Cybersecurity is necessary for the survival of your business in the world of today. Get started on your journey to cybersecurity with the vital tips shared in this post.

https://www.entrepreneur.com/article/355861

Attacco hacker al Gruppo Carraro, CIG per i 700 dipendenti delle sedi italiane

Il Gruppo **Carraro,** azienda leader internazionale nel comparto

delle macchine agricole che conta oltre tremila dipendenti in tutto il mondo e un fatturato che sfiora i **550 milioni,** ha subito un grave attacco informatico nella giornata di martedì.

Imprese del Veneto e cybercrime: dopo Luxottica il Gruppo Carraro

L'attacco, sicuramente un altro ransowmare come quello subito dalla **Luxottica** pochi giorni fa, ha paralizzato i sistemi informatici che controllano praticamente tutta l'attività del gruppo, da quella amministrativa a quella produttiva, altamente automatizzata da robot.

L'azienda ha dovuto mettere settecento dipendenti in cassa integrazione tra gli stabilimenti di Campodarsego e quelli della divisione Agritalia di Rovigo in attesa del ripristino dei sistemi.

"Per i collaboratori italiani che in queste ore non potessero garantire la propria prestazione lavorativa l'azienda ha provveduto precauzionalmente all'attivazione della Cassa Integrazione", si legge nella nota diffusa dal Gruppo diffusa ieri. *"Inoltre sono state attivate le coperture assicurative dedicate a questa tipologia di evento*".

La buona notizia, fa sapere l'azienda, è che la tempestiva attivazione dei sistemi di difesa IT ha consentito di respingere l'attacco dei criminal hacker impedendo l'accesso e la conseguente sottrazione di dati e informazioni riservate.

Nessun furto di dati

"A scopo precauzionale, continua la nota, *alcune attività degli uffici sono state temporaneamente interrotte, mentre per altre sono state attivate procedure alternative di connessione. I reparti produttivi hanno proseguito la propria programmazione adattandosi alle previste procedure analogiche*

di backup.

“Il Dipartimento IT Carraro è prontamente entrato in azione, anche con la collaborazione di esperti in materia e con le forze dell’ordine, allo scopo di verificare possibili danni all’infrastruttura nonché di valutare eventuali azioni di bonifica della rete di server interessati dall’attacco. Si prevede – conclude la nota – *che dalla giornata di domani e nei prossimi giorni le attività tornino progressivamente a regime”.*

I problemi recenti con la sicurezza informatica

Nell’ultima settimana in Veneto hacker sconosciuti che stanno mandando in tilt i sistemi informatici di aziende e anche i social network di leader politici.

L’ultima, in ordine temporale, è stata **Luxottica**, la più grande produttrice mondiale di montature per occhiali da vista e da sole. L’attacco ha causato la sospensione del secondo turno produttivo negli stabilimenti di **Agordo** e Sedico, nel bellunese, e il blocco delle attività produttive in Cina. Per fortuna anche lì l’azienda guidata da **Leonardo Dal Vecchio** è riuscita ad attivare le difese IT per proteggere i propri dati aziendali.

Anche il Governatore del Veneto **Luca Zaia**, aveva denunciato attacchi informatici ai suoi profili social poche ore prima del voto per le Regionali 2020.

A giugno invece la vittima è stata **Geox**, azienda trevigiana di calzature. dove anche lì un ransomware ha colpito i sistemi IT dell’azienda.

Dalla logistica, all’eCommerce, passando pure per le email aziendali, tanto che molti dei lavoratori dell’headquater di Montebelluna (TV) sono stati lasciati a casa per due giorni.

https://www.key4biz.it/attacco-hacker-al-gruppo-carraro-cig-per-i-700-dipendenti-delle-sedi-italiane/322753/

---

eCommerce, data breach per Shopify. Due ex dipendenti rubano dati di 200 clienti

Shopify, il colosso canadese che sviluppa e commercializza l'omonima piattaforma di eCommerce in tutto il mondo, ha confermato una violazione dei dati.

In un post sul blog ufficiale, la società ha reso noto che le informazioni relative ai clienti di circa 200 commercianti iscritti alla piattaforma potrebbero essere state esposte. È la conseguenza dell'azione malevola perpetrata da due ex dipendenti intenzionati a rubare informazioni riservate.

L'azienda, che ha denunciato subito l'accaduto all'FBI, ha dichiarato che "*l'incidente non è stato il risultato di una vulnerabilità tecnica nella nostra piattaforma e la stragrande maggioranza dei commercianti che utilizzano Shopify non è risultata interessata*".

Data breach Spotify: cosa è successo

Secondo il post, i negozi interessati potrebbero aver esposto i dati dei consumatori, inclusi indirizzi e-mail, nomi,

indirizzi e altre informazioni pertinenti. Shopify ha affermato di non avere prove che suggeriscano che i dati siano stati utilizzati, ma di aver informato i commercianti interessati dell'incidente.

Secondo quanto riferito da Bloomberg, **Ric Kostick,** CEO di **100% Pure**, uno dei 200 rivenditori vittima del data breach, ha dichiarato: *"La violazione è avvenuta il 15 settembre. La massima priorità dell'azienda in questo momento è garantire che la sicurezza e la protezione dei propri dati siano protette. Stiamo valutando attentamente l'entità di questo incidente con Shopify e adotteremo tutte le azioni necessarie e immediate per evitare che ciò accada di nuovo."*

Shopify: 33 miliardi di dollari di fatturato

Shopify negli ultimi mesi ha visto un'impennata dell'attività grazie alla pandemia da Coronavirus che ha costretto tanti rivenditori passare al digitale.

Nel secondo trimestre di quest'anno, Shopify ha registrato un fatturato di 714,3 milioni di dollari, con un aumento del 97 percento rispetto allo scorso anno. Il volume lordo delle merci è aumentato del 119%, con aumenti particolari in aprile e maggio. Attualmente il valore di Shopify è di 33 miliardi di dollari.

Cybersecurity e minacce interne

Secondo gli ultimi dati contenuti nel Data Breach Investigations Report di Verizon, il 20% degli incidenti legati alla cybersecurity e il 15% delle violazioni dei dati provengono da soggetti interni all'organizzazione.

Tuttavia, per molte organizzazioni le minacce interne rimangono un argomento tabù.

Gli esperti evidenziano come le aziende si mostrano troppo spesso restie a riconoscere, segnalare o intraprendere azioni contro i dipendenti che sono diventati una minaccia per la loro organizzazione. È come se una minaccia interna fosse una macchia sui loro processi di gestione e sul loro nome.

Secondo il report sono state individuate cinque personalità che possono minacciare un'azienda dall'interno: il lavoratore distratto, l'agente infiltrato, il dipendente insoddisfatto, la risorsa interna malintenzionata e la terza parte incompetente.

https://www.key4biz.it/ecommerce-data-breach-per-shopify-due-ex-dipendenti-rubano-dati-di-200-clienti/322585/

Traffico di armi e droga nel Dark Web, 179 arresti nell'operazione DisrupTor

Una coalizione di forze dell'ordine europee e americane ha arrestato 179 criminali ritenuti responsabili di traffico di droga e armi nel Dark Web.

Secondo un comunicato diffuso dall'Europol, l'operazione, denominata **DisrupTor**, ha portato al sequestro di 6,5 milioni di dollari sia in contanti che in valute virtuali, insieme a circa 500 chilogrammi di droghe, tra cui fentanil, ossicodone, idrocodone, metanfetamina, eroina, cocaina, ecstasy, MDMA e 64 armi da fuoco.

I dettagli dell'operazione DisrupTor

L'operazione **DisrupTor** era composta da una serie di operazioni congiunte separate ma complementari coordinate da **Europol** ed **Eurojust**, in collaborazione tra le forze dell'ordine e le autorità giudiziarie di Austria, Cipro, Germania, Paesi Bassi, Svezia, Australia, Canada, Regno Unito e Stati Uniti.

> *ONCE UPON A TIME ON THE DARK WEB…*
>
> *Police authorities from 9 countries set out on a journey to catch cybercriminals coordinated by @Europol and @Eurojust*
>
> *179 vendors were arrested.*
> *$6.5m and 500kg of drugs were seized.*
>
> *Want to know the whole story? https://t.co/6H4ErdGieP pic.twitter.com/1ci8rz5ZUT*
>
> *— Europol (@Europol) September 22, 2020*

Gli arresti sono stati effettuati negli Stati Uniti (121), in Germania (42), nei Paesi Bassi (8), nel Regno Unito (4), in Austria (3) e in Svezia (1). Sono ancora in corso numerose indagini per identificare le persone dietro gli account del dark web, si legge nella nota dell'Europol.

"Le forze dell'ordine sono più efficaci quando collaborano e l'annuncio di oggi lancia un forte messaggio ai criminali che vendono o acquistano beni illegali sul Dark Web: la parte di Internet che credete nascosta non lo è più e le vostre attività non sono più anonime. Siamo impegnati nel tracciare i criminali, non importa dove si trovino, nelle strade o dietro lo schermo di un computer.", ha dichiarato **Edvardas Šileris**, capo del Centro europeo per la criminalità informatica (EC3) di Europol.

Cybercrime: tra ransomware e dark web

Nonostante l'impegno delle forze dell'ordine, il cybercrime non accenna a placarsi, anzi, nel 2020 si è evidenziato un aumento di crimini informatici.

Un risultato legato anche all'aumento considerevole delle persone che lavorano e studiano da casa, per via dell'epidemia di Covid-19, ma con le solite scarse protezioni informatiche e una maggiore esposizione ai cyber criminali.

Nel nuovo studio pubblicato da Immuniweb, dal titolo "***Cybersecurity Industry Exposure at Dark Web***", nel 2020, il 59% delle imprese ha sofferto di azioni di *data breach*, con il risultato che 15 miliardi di record di dati, provenienti da oltre 100 mila incidenti informatici, sono finiti in vendita nel dark web.

Durante i primi 7 mesi dell'anno in corso, sempre secondo il Report, **s**i sono registrati 631.512 incidenti informatici, di cui 160.529 classificati come "*critici*".

Ransomware e aziende

Le aziende, in questo 2020, sono state colpite duramente dai criminal hacker. L'ultima, in Italia, è stata **Luxottica**, la più grande produttrice mondiale di montature per occhiali da vista e da sole.

L'azienda bellunese è stata vittima di un grave attacco ransomware ai propri sistemi informatici che ha bloccato l'intera produzione nelle sedi di **Agordo e Sedico**.

Per fortuna, seconda fonti sindacali, l'azienda è stata in grado di respingere l'attacco impedendo l'accesso e la conseguente sottrazione di dati e informazioni riservati su

utenti, consumatori e proprietà intellettuali dell’azienda.

https://www.key4biz.it/traffico-di-armi-e-droga-nel-dark-web-179-arresti-nelloperazione-disruptor/322461/

Banda del ransomware ruba dati sensibili di 540 mila arbitri sportivi negli Stati Uniti

Breccia nel sistema di difesa informatica di una società che fornisce software gestionali per la **NCAA** (*National Collegiate Athletic Association*), la lega nazionale degli arbitri, dei giudici e degli ufficiali delle varie leghe e discipline sportive negli Stati Uniti.

Secondo quanto riferito ai media dal provider stesso, **ArbiterSports**, nei giorni scorsi, la *software company* è riuscita a respingere un **attacco ransomware**, ma non ad evitare il ***data breach***.

La cyber banda ha effettuato una copia dei *backup* e quindi dei dati di tutti gli arbitri e giudici sportivi registrati alla NCAA.

In tutto **dovrebbero essere 540 mila gli utenti coinvolti dal cyber attacco**.

Un bottino classico, fatto di dati sensibili, come indirizzi

di casa, numero di previdenza sociale, carte di pagamento, password, indirizzi email, account vari e anche licenze di guida.

ArbiterSports, dopo aver subito l'attacco, si è vista recapitare una richiesta di riscatto, tipico di un ransomware. In cambio del pagamento, i cyber criminali avrebbero distrutto tutti i dati sottratti, altrimenti li avrebbero offerti sui mercati del ***dark web***.

La società ha deciso di pagare il riscatto e la banda del ransomware ha assicurato che i dati sarebbero stati eliminati.

Il problema è: ci si può fidare?
Si può stare sicuri che i cyber criminali nel frattempo non abbiamo eseguito copia dei dati in questione?

Troppo spesso situazioni del genere hanno dimostrato che i dati, una volta rubati, quasi sempre finiscono sul mercato nero del web.

Secondo un nuovo report diffuso da Coalition, il 41% degli attacchi sferrati contro il settore delle assicurazioni online in Nord America, nella prima metà del 2020, è di tipo ransomware, con un incremento del +260% rispetto all'anno passato.

> *Banda del ransomware ruba dati sensibili di 540 mila arbitri sportivi negli Stati Uniti*

Attacchi informatici contro i canali social della Azzolina: “Non ci spaventiamo”

Da 48 ore i profili social della ministra dell’Istruzione, **Lucia Azzolina**, sono sotto attacco informatico.

È quanto annunciato dalla Azzolina stessa in un post su Facebook e un tweet su Twitter.

“*Da due giorni i miei profili social e le strutture informatiche del Ministero dell’Istruzione sono bersaglio di attacchi da parte di un gruppo di pirati informatici*”, ci tiene ha precisato Azzolina.

“*Non ci spaventiamo e non ci faremo fermare neanche da questo tipo di aggressioni*”, ha dichiarato perentoriamente.

Il messaggio si conclude con il ringraziamento alla Polizia Postale “*per la rapidità e la professionalità con cui sta gestendo questa vicenda*”.

> *Non ci spaventiamo e non ci faremo fermare neanche da questo tipo di aggressioni.*
> *Un ringraziamento alla Polizia Postale per la rapidità e la professionalità con cui sta gestendo questa vicenda.*
> *pic.twitter.com/jHNIzryCuT*
>
> *— Lucia Azzolina (@AzzolinaLucia) September 18, 2020*

Obiettivo dei cyber criminali, secondo quanto riportato dall’*huffintonpost.it*, è violare il database del ministero dell’Istruzione, dell’università e della ricerca per sottrarre

dati sensibili.

Da ieri sono in corso decine di tentativi di data breach, di furti di identità e di introdursi nei profili social, negli account di posta elettronica e nelle stesse strutture informatiche del ministero.

Le indagini della Polizia Postale sono partite subito e secondo fonti ben informate si attende nelle prossime ore una nuova ondata di attacchi informatici dello stesso tipo verso gli stessi obiettivi.

> *Attacchi informatici contro i canali social della Azzolina: "Non ci spaventiamo"*

Primo omicidio causato da hackeraggio di un ospedale

Una donna in gravi condizioni è arrivata alla clinica dell'università di Dusseldorf, ma il pronto soccorso era stato chiuso a causa di un attacco hacker, così è stata dirottata a Wuppertal, a circa 30 chilometri di distanza, con un ritardo di un'ora nelle cure. Il tentativo è stato vano: la donna è poi deceduta.

La procura di Colonia ha aperto un'indagine per omicidio colposo aggiungendo di poter ritenere gli hacker colpevoli del reato. Un esperto del settore ha rivelato che se fosse confermato sarebbe il primo caso di un omicidio come risultato di un hackeraggio.

L’attacco hacker era stato effettuato nella notte del 9 settembre e il ransomware aveva reso l’intero sistema di computer dell’ospedale completamente non operativo.

Secondo le prime ricostruzioni, gli hacker non intendevano colpire l’ospedale ma una università.

Infatti, il messaggio lasciato su uno dei server chiedeva il riscatto, di circa 900mila euro pagabili in bitcoin, all’università Heinrich Heine, affiliata all’ospedale, e non all’ospedale stesso.

La polizia di Dusseldorf ha quindi contattato gli hacker spiegando loro che avevano colpito l’ospedale e non l’università: così i cybercriminali hanno ritirato la richiesta fornendo la chiave per decrittare i dati.

“Le indagini – hanno spiegato le autorità – *sono ancora in corso per stabilire se c’è un nesso tra la morte e l’attacco, che se provato potrebbe far cambiare il capo di imputazione per gli autori del gesto”.*

Autori dell’attacco hacker che andrebbero così cacciati nel dark web. Tuttavia, l’incidente, che probabilmente avrebbe causato la morte della donna, fa emergere un nuovo problema da risolvere nella sanità: si può morire ora anche a causa di una cattiva gestione della sicurezza informativa nella sanità.

Potrebbero essere indagati sia il direttore generale dell’ospedale sia il responsabile della cybersecurity perché non in grado di difendere l’ospedale dall’attacco hacker?

Oggigiorni per i pazienti nelle strutture sanitarie sono necessari:

oltre alle buone cure, anche un’infrastruttura informatica sicura.

Primo omicidio causato da hackeraggio di un ospedale