FEB 2019

THREATSPLOIT ADVERSARY REPORT

Edition - 6

PREPARED BY

B115 NM ROAD, CHENNAI, INDIA -94
044 4352 4537 / +91 8608634123

www.briskinfosec.com
contact@briskinfosec.com

“Everyone fight’s for data’s safety
We spend more towards cyber security
Nevertheless, we are hacked beyond cyber guarantee”!

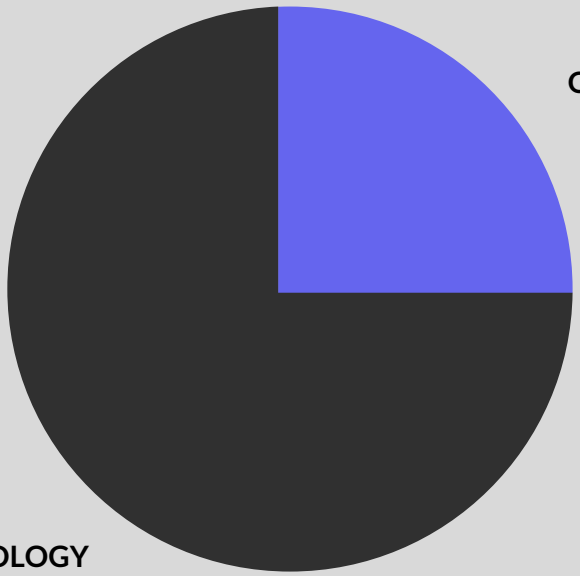
The last couple of years has been a rough tide for cybersecurity professionals to surf on as multiple financial heists to various distinct organizations, situated both in the Asia-pacific region as well as in the other parts of cosmos, have been breached.

On this 6th edition we have consolidated the major cyberattacks of last-month for your learning and reference. We have done this to notify you about the horrendous catastrophes these cyber breaches are capable to cause persons, as well to your organizations.

Most significantly, this is done because we as cybersecurity folks truly care for your digital safety.

DATA STATISTICS OF JANUARY

Among the various cyber incidents reported, it's the technical sector that is leading the breached list. The humongous count of Information technology appliances being hacked, to believe are fainting. But after striking reality, people experience gravity due to bewilderness of hopes. Moreover, the saddest and defying part is that, these breaches continue to increase and shows zero signs of decrease.



CONTENT TABLE

TECHNOLOGY

- Abine Blur Password Manager suffers a data breach exposing private data of 2.4 million users.
- Kenya's Communication Authority issues an alert on detection of Emotet Trojan.
- BlackMediaGames hacked resulting in the compromise of over 7 million accounts.
- Security researchers report the latest Emotet campaign's propagation technique.
- Ehereum Classic (ETC) Hit by Double-Spend Attack Worth $1.1 Million.
- Nasty Side-Channel Attack Vulnerability (Again) In Windows & Linux Discovered.
- Attacks Targeting Recent PHP Framework Vulnerability Found.
- .Chinese Hacker Publishes PoC for Remote iOS 12 Jailbreak On iPhone X.
- Critical RCE Flaw in Linux APT Allows Remote Attackers to Hack Systems.
- Unprotected Government Server Exposes Years of FBI Investigations.
- Hackers infect e-commerce sites by compromising their advertising partner.
- Flight Booking System Flaw Affected Customers of 141 Airlines Worldwide.
- Fortnite Flaws Allowed Hackers to Takeover Gamers' Accounts.
- Unprotected VOIP Server Exposed Millions of SMS Messages, Call Logs.
- 5 Popular Web Hosting Services Found Vulnerable to Multiple Flaws.
- 36-Year-Old SCP Clients' Implementation Flaws Discovered.
- Unpatched vCard Flaw Could Let Attackers Hack Your Windows PCs.
- Over 202 Million Chinese Job Seekers' Details Exposed On the Internet.
- New Systemd Privilege Escalation Flaws Affect Most Linux Distributions.
- Hackers Using Zero-Width Spaces to Bypass MS Office 365 Protection
- Turns Out Kaspersky Labs Helped FBI Catch Alleged NSA Leaker.
- The WhatsApp Gold Scam is Back, in a New Form!
- Google DNS Service (8.8.8.8) Now Supports DNS-over-TLS Security.
- Scamvertisers using Botnets and Public Servers for Hire, Charged in New York.
- Life under GDPR: Data Breach Cost Unknown.
- New Exploit Kit "Novidade" Found Targeting Home and SOHO Routers.
- Internet-of-Things (IoT) Security: Developments in VPN Filter and Emergence of Torii Botnet.

HEALTHCARE

- Alaska Bungles Breach Notification, 87,000 Patients Impacted.
- Months-Long Phishing Attack on Rehab Center Breaches Patient Data.
- Third-Party Vendor Phishing Attack Breaches 31,000 Patient Records
- Hackers Breach Data of 4,300 Missouri Patients for 3 Months.
- Zero-Day Virus Forces EHR Downtime at 21 Health Science North Hospitals.
- Healthcare Organizations Falling Behind on Cyber Risk Management.

FINANCE

- 4-Month Breach of BenefitMall Impacts 112,000 Plan Members.
- Phishing Attack Hits Kent County Community Mental Health.
- Ukrainian Police Arrest 6 Hackers Linked to DDoS and Financial Attacks.

RANSOMEWARE

- Ransomware Corrupts 24,000 Patient Records of California Specialist.
- Irish Tram Operator Website Hacked For Bitcoin Ransom.
- Ransomware: A Pervasive, Evolving Threat.
- PyLocky Ransomware Decryption Tool Released — Unlock Files For Free.

TECHNOLOGY

Abine Blur Password Manager suffers a data breach exposing private data of 2.4 million users

Various significant information like email addresses, first and last names, last and second-to-last IP addresses were left exposed.

Abine Blur Password Manager suffers a data breach exposing private data of 2.4 million users Significant information's like email addresses, first and last names, last and second-to-last IP addresses were left exposed. These data's were used to login to Blur and also to encrypt those passwords. Blur finalized that there was zero evidence for the exposure of usernames and passwords, auto-fill credit card details, masked emails, masked phone numbers, masked credit card numbers and payment details. On 31st December 2018, an online privacy company named as Abine that owns Blur and DeleteMe, figured out the online exposure of Blur password manager users. Blur became aware of this incident on 13 December, 2018 and post it, Blur firm instantly began to work on investigating the issue and for confirming the certainty of their data's and systems security. After the ending of investigation, it was revealed on Monday that "A file containing information from users who had registered prior to January 2016 were exposed online". Blur is collaborating with a leading security firm to prevent the existence of breaches in future.

Attack Type	Cause Of Issue	Type Of Loss	Country
Phishing attack	Lack Of awareness	Money/data	USA

Kenya's Communication Authority issues an alert on detection of Emotet trojan

The usage of a Trojan named as Emotet for performing attacks on local organizations

The usage of a Trojan named as Emotet for performing attacks on local organizations has been done on 11 instances, fragmented and attached through malicious email attachments v - detects the National KE-CIRT/CC. The Communication Authority of Kenya (CA) cautioned its residents of an advanced, catastrophic banking malware that targets the network systems. This Emotet malware has damaged several firms.

Propagation

General Tom Olwero - The CA director says other than dissemination of malware through mail, it is also posted through phishing techniques that appears to be from legal links like invoices, from banks and much more. Further, Olwero said that," Emotet is modern and a malicious Trojan as its modular design, persistence techniques and worm-like self-propagation steadfastly spread infection to wide networks", the Star reported. It is also said that if it's once injected, then the systems will be infected. The malware seems to be a frightening threat to Kenyan firms as it can cause the significant loss of temporary/permanent files for an organization, obviously leading to reputation dash. About the potentialities of Trojan, Olwero commented that "it can dodge typical signature-based detection and has various ways for maintaining persistence that includes the functions of auto-start registry keys and its services", says the Standard report.

Attack Type	Cause Of Issue	Type Of Loss	Country
Ransomware	Lack Of Awareness	Data/reputation	Kenya

TECHNOLOGY

BlackMediaGames hacked resulting in the compromise of over 7 million accounts

The developer of an online browser based game, situated in the 'Town of Salem' has suffered a data breach that compromised over 7 million user data's

On 28th December 2018, BlackMediaGames - the developer of an online browser based game, situated in the 'Town of Salem' has suffered a data breach that compromised over 7 million user data's. A faulty email was received by Dehashed (a Data-Mining and hacked database search engine) that surmounted the evidence of server access as well the details of the exposed database. Post this mail, it was lucid that Dehashed has been breached. A faulty email was received by Dehashed (a Data-Mining and hacked database search engine) that surmounted the evidence of server access as well the details of the exposed database. Post this mail, it was lucid that Dehashed has been breached. Types of information compromised
The affected User's data's comprised of various usernames, emails, passwords, IP addresses, Game and Forum activities, payment information as well as the Billing information of users for certain premium features were also impacted. This is first time BlackMediaGames has been breached by cyberattacks. As a cybersecurity awareness move, Dehashed has informed the firm about the email attack. Dehashed has given the data's to HaveIBeenPwned. It is a search engine that keeps track of the compromised email accounts. For preventing further threats, the firm is collaborating with many security researchers to reduce similar breaches.

Attack Type	Cause Of Issue	Type Of Loss	Country
phishing attack	Lack OF Awareness	Data/Money	Town Of Salem

Security researchers report the latest Emotet campaign's propagation technique

cybercriminals have utilised the Microsoft Office suite to propagate their threats from simple macros merged in files for the exploitation of vulnerabilities

Of late, cyber criminals have utilized the Microsoft Office suite to propagate their threats from simple macros merged in files for the exploitation of vulnerabilities. On this occasion, implementation of a down-loader was incorporated into an office file. This aroused some chaos among readers who asked to demonstrate how the threat works- published by ESET. Attack initiated through a phishing email with a malicious attachment. After downloading and opening, it will ask the victims to enable the macros. The trick used by hackers in this campaign is equipped with strange features as macro doesn't attempt to connect a website for downloading malicious content. In top left corner, appears a small, square and solid expandable box, after which it contains a "cmd" command that uses Power-Shell script for persuading to connect five sites. This is done for downloading the payload, and an overshadowed variant named as Emotet. The payload gets connected to the C2 server after it gets executed. It can attempt further downloads by installing attack modules and secondary payloads for performing malicious deeds on systems.
"The prospect at which this Emotet Trojan is hidden within a word file shows the stealthy intellect of cyber-criminals in launching attacks, in a bid to compromise the user information of the victims system"- ESET concluded.compromise the user information of the victims system"- ESET concluded.

Attack Type	Cause Of Issue	Type Of Loss	Country
phishing attack	Lack Of Awareness	Data	USA/UK

TECHNOLOGY

Ethereum Classic (ETC) Hit by Double-Spend Attack Worth $1.1 Million

Coinbase revealed on Monday that it found "a deep chain reorganization" of the Ethereum Classic Block chain

Coinbase revealed on Monday that it found "a deep chain reorganization" of the Ethereum Classic Block chain, which means that someone controlling the majority of miners on the network, had modified the transaction history. Coinbase detected the deep chain reorganization of the Ethereum Classic blockchain on 5th January, at which point the organization settled on-chain ETC payments for safeguarding its customer funds and the cryptocurrency exchanges. Initially, Coinbase found nine reorganizations had contained double spends that costs up to 88,500 ETC (about $460,000), but the latest update on its blog post tells us that at least 12 additional reorganizations included double spends, that totalled up to 219,500 ETC, which ranges to nearly $1.1Million.

However, Ethereum Classic refused the claim that Coinbase contacted ETC personnel about the attack. Since it is highly tangent to mount such attacks against heavily-mined cryptocurrency networks such as Bitcoin and Ethereum, hackers chose to target small-cap cryptocurrencies like Ethereum Classic, Litecoin Cash, Bitcoin Gold, ZenCash (now Horizen), and Verge. Having its inception in June 2016, Ethereum Classic is the 18th-largest cryptocurrency containing a market cap of more than half a billion dollars (around $539 million), that makes it a luring deal for hackers to attack.

Attack Type	Cause Of Issue	Type Of Loss	Country
Cryptominning	Unsecured network	Data/Money	Japan

Nasty Side-Channel Attack Vulnerability (Again) In Windows & Linux Discovered

A new variant of side-channel attack was detected of late that is actively pilfering the data's of Windows and Linux targets

A new variant of side-channel attack was detected of late that is actively pilfering the data's of Windows and Linux targets. Side-channel attacks are secondary choice exploitation scenarios of a system through cache, acoustic, electromagnetic, sound, power or timing information. Both Microsoft and Linux teams were acknowledged about the issue presented in the paper, and all of their data leaks have known the mitigation procedures as implemented by both Microsoft and Linux teams. This usually comes as an update to both Linux and Windows core system files and libraries for alleviating the issues brought forth by the paper's authors. The boon of the tracked side-channel attack is the quantity of original data that can be regained, with a spatial resolution of 4KB. Data leakage is obviously the ultimate goal for any attacker who tries to flawlessly execute such type of attack. With 4KB information per two microseconds is shockingly but truly a humongous amount of information extraction than the notorious keystroke logger attack. It basically means the attack will be able to excavate information from a system as instant as 6 keystrokes per second. To your surprise, it is as fast as the world's fastest typist.

Attack Type	Cause Of Issue	Type Of Loss	Country

TECHNOLOGY

Attacks Targeting Recent PHP Framework Vulnerability Found

Chinese company developed a rapid-development framework named as ThinkPHP, in which the existence of a vulnerable code was identified

Top Think, a Chinese company developed a rapid-development framework named as ThinkPHP, in which the existence of a vulnerable code was identified, last month. "Multiple threat actors are in a pursuit to exploit ThinkPHP vulnerability to initiate cryptominers, skimmers and other malware payloads"- says Larry Cashdollar, a vulnerability researchers after he was researching on a recent Magecart attack. During this phase, he noticed the wobbling presence of a malware which was something unseen in the past.The developers resolved the vulnerability indicating that," The framework doesn't detect the controller name which may lead to potential 'getshell' vulnerabilities without forced routing enabled". This vulnerability has been assigned as CVE-2018-20062. Parallel to the observance of many payloads, Larry Cashdollar found something that is a matter of concern named as 'Mirai Variant'. The Dark Reading report quotes Cashdollar as saying," I had been waiting for Mirai botnet kits for including Web app codes in their storage and is a premonition that it's happening". Cashdollar further says that, "Unlike the threat actors in 1990 persuading to gain root access, the current threat actors just execute a code pretending as a legitimate user and surreptitiously spreading malware and botnet for mining cryptocurrency. Their primary notion is to run the code on a large systems count. Apart from threat actors scanning software firms and car rentals, there are more than 600 scans happening per day. As a factor of security betterment, firms using ThinkPHP framework must update to the latest version without delay.

Attack Type	Cause Of Issue	Type Of Loss	Country
Think PHP Framework Attack	Malware	Data/Money	China

HEALTH CARE

Alaska Bungles Breach Notification, 87,000 Patients Impacted

A new variant of side-channel attack was detected of late that is actively pilfering the data's of Windows and Linux targets

On 25th January 2019, the update on breach notification was recently done by the Alaska Department of Health and Social services for including more number of patients than in its initial announcement, from June 2018. In this process, these speculations later proved incorrect. Between 2018 26th April and 30th April, a malware has attacked a possible database that comprised patient names, Social Security numbers, benefit information, dates of birth, addresses and other personal details-says DHSS. The hack occurred at the time when an applicant emailed a request for assistance to DHSS for a state employee. As emails are sent through attractive displays, the employee opened the malicious file that had Zeus/Zbot Trojan. The hackers then installed the malicious software and performed "other suspicious computer behaviour". Hackers infiltrated into the laptop's hard drive with "Day One" virus that spread before the DHSS IT team could stop it. As for the delayed notification, officials said that the investigation included a mass volume of data which consumed months. The FBI still haven't identified the source. Hackers primary target have been the Healthcare and Government sectors as they had suffered most breaches recently. Of late even, Kent County Community Mental Health notified about 2,200 patients potential data's have been breached.

Attack Type	Cause Of Issue	Type Of Loss	Country
Side channel attack	insecure database	Data/Money	Alaska

HEALTH CARE

Months-Long Phishing Attack on Rehab Center Breaches Patient Data

Memphis-based Sacred Heart Rehabilitation Center notified patients that a phishing attack has potentially breached many users personal data

On 17th January 2019, Memphis-based Sacred Heart Rehabilitation Center notified patients that a phishing attack has potentially breached many users personal data between 5th and 7th April, after a hacker gained the employee email access. Officials didn't comment when the breach was discovered. The investigation concluded in November. The breached data's included patient names, Social Security numbers, health insurance information, treatment details, diagnoses and much more. Sacred heart has improved its security features through security awareness training for employees. The breach wasn't listed in the department of Health and Human services. Hence, all patients are offered a year of free credit monitoring. Patients receiving treatment at the Hanger Clinic in Florida are notified about the finding of patient records at the home of a former clinic employee's ex-spouse. The individual returned the box to the Hanger Clinic. It is believed that the patient's records were stored at home in 2009 and 2014, when an employee stopped to work at the clinic. The records contained patients data's whom received care at hanger clinic in 2009. The individual signed that he didn't access the box contents. As a precaution, we recommend the individuals to review the benefits statement received from his health insurer, officials said. If the individual didn't receive the benefits listed on the benefits list, then the individual must contact his insurer.

Attack Type	Cause Of Issue	Type Of Loss	Country
phishing attack	Lack of awareness	Data/Money	USA

Finance

4-Month Breach of Benefit Mall Impacts 112,000 Plan Members

A Centerstone Insurance and Financial services firm informed about the breach of 111,589 personal data to customers due to phishing attack

On 15th January 2019, Benefit Mall- A Centerstone Insurance and Financial services firm informed about the breach of 111,589 personal data to customers due to phishing attack. On 11th October, officials found that the hacker through the usage of phishing technique has gained the control of various systems. A third party forensics team was hired, with the investigation consuming 4 months period. During investigation phase, it was confirmed that the breached data's included names, Social security numbers, bank account numbers, insurance premium payment information, date of birth and addresses. As a boon move, benefit mall has implemented two-factor authentication (2FA) with proper training on phishing awareness. Notifications were sent to all on 4th January by the officials but no explanation on the reason for delay in reporting this since October 11th. Under HIPAA, healthcare organizations must report the breaches within 60 days of discovery. Most recently, Choice Rehabilitation Center informed 4,300 patients of a phishing hack on an employee email account. This list includes TandigmHealth, San Diego School district and Health first. The best possible method to detect unauthorized access is through access management and network monitoring. As threats continue to improve in sophistication, shielding up user authentication issues will be crucial for healthcare sector.

Attack Type	Cause Of Issue	Type Of Loss	Country
Phishing attack	unsecured server	Data/Money	USA

Phishing Attack Hits Kent County Community Mental Health

Kent county community Mental Health Authority that their data's were breached,

On 10th January 2019, 2284 patients were informed by the Kent county community Mental Health Authority that their data's were breached, due to a spiral of phishing attacks. After a 9 day investigation by various HIPAA privacy officer, HIPAA security officer and by the IT department, the officials confirmed that the phishing attacks on October 28th have victimised three employees email accounts. The breached accounts contained in the email included names, addresses, dates of birth, Medicaid and Medicare ID numbers, waiver support application ID numbers, provider names, schools attending or attended, demographic data and the names of relatives. Social Security numbers of 20% patients have also been compromised. As a remedy, mass password reset and additional safeguarding techniques were done to ensure none other accounts get hacked.

THEFT OF UNENCRYPTED LAPTOP BEHIND SOLIS MAMMOGRAPHY BREACH

Solis Mammography reported the abduction of an unencrypted laptop on October 18 from its Phoenix, Arizona clinic to 500 patients. The investigation determined it's impossible to figure out what data was exposed. Through the help of forensic team, it was figured out that patient names, birth names, health insurance data, lab results, medical images and PII were exposed. Nevertheless, justified explanation about the presence of unencrypted data's on laptop, remains still unjustified. Since then, Solid Mammography have hardened their security features.

Attack Type	Cause Of Issue	Type Of Loss	Country
Phishing attack	Network security Flaw	Data/Money	USA

Third-Party Vendor Phishing Attack Breaches 31,000 Patient Records

Health Services of Indiana Health Plan cautioned 31,000 patients personal data breach, with phishing attacks the causality.

On 9th January 2019, Health Services of Indiana Health Plan cautioned 31,000 patients personal data breach, with phishing attacks the causality. As per the officials, LCP Transportation employees through MHS vendor responded to phishing emails on 30th July which gave hackers remote access to accounts over a month. Post this acknowledgement, LCP isolated the impacted accounts on September 7th. Investigation by forensics team made it evident that patient data's like names, insurance ID numbers, addresses, date of birth, dates of service and other were exposed. LCP Transportation informed the breach to MHS on Oct 29th. Post this, MHS hired its own enquiry on this issue till December 20th. "Our vendor is making necessary betterments for strengthening the security defences. Simultaneously, patients will be also provided a year of free credit monitoring. Apropos to it, MHS on the same day cautioned patients of another 3rd party hack on Oct 16th, due to a mailing error which resulted in the disclosure of health information. Officials learnt about this on 25th Oct and revealed that the information contained names, insurance ID's, of about 576 plan members. As a remedy, MHS is calling patients to retrieve the letter mailed to wrong recipients. Further, Officials are revamping the mailing policies and procedures around patient data while simultaneously reviewing the process of sending mails

Attack Type	Cause Of Issue	Type Of Loss	Country
phishing attack	Network Flaw	Data/Money	USA

Ransomware

Ransomware Corrupts 24,000 Patient Records of California Specialist

A ransomware attack has corrupted the medical records of 24,000 patients on the Podiatric Offices of Bobby.

On 7th January 2019, a ransomware attack has corrupted the medical records of 24,000 patients on the Podiatric Offices of Bobby. Typically, ransomware encrypts the data's on the infected host. The affected data's included patient names, Social Security numbers, health insurance policy details, medical records, date of birth, phone numbers, sex and addresses. "Once we acknowledged the incident, needed steps to safeguard your passwords have been activated. Further, if any alteration of your personal info is to be made, we need to reconstruct the information that is inclusive of your medical information"- said Officials.

THIRD HEALTH DATA BREACH FOR HUMANA IN DECEMBER

A business associate for Humana names as Banker's life informed the health insurer on 25th Oct that a hacker has accessed and seized the credentials of few employees where consumers claim for Humana health insurance. As per reports, the cyber conman has accessed the site in the midst of 30th May to 13th September. On August 7th, Bankers life found out "unusual activity". Post this, they hired an external forensics team and figured out that hackers had accessed applicant names, addresses, date of birth, social security numbers, health insurance policy details like policy numbers and its cost. Since then, Officials have taken measures to restrict unauthorized system access.

Attack Type	Cause Of Issue	Type Of Loss	Country
Ransomware	Lack of nearness	Data/Money	USA

HEALTHCARE

Hackers Breach Data of 4,300 Missouri Patients for 3 Months

Patient's data were breached on a corporate email- reports Missouri based rehabilitation Center named as 'Choice'

On 3rd January 2019, 4,309 patient's data were breached on a corporate email- reports Missouri based rehabilitation Center named as 'Choice'. On 7th November, Choice identified one of its hacked email account. As per officials, cybercriminals forwarded the provider's email to their personal account. The account was later deactivated. Choice negotiated with Microsoft and initiated an investigation about the attack. The investigation revealed that hackers had accessed the accounts from 1st July to 30th September. They have compromised data's that encompassed patient names, medical record numbers, treatment facility, Medicare data, beginning and end of treatment dates, treatment information, diagnosis and billing codes. These are the data's which are frequently and fervently utilised by cybercriminals for medical fraud. Choice is teaming up with its contracted nursing facilities for notifying patients and for alleviating the possible hazards that could be caused by the breach. Since then, officials have concentrated their network security defences and are simultaneously improving their operation security as well as in providing training to employees. The previous month, Philadelphia based Independence Blue Cross declared that a breach was present for 3 months because of an employee error.

Attack Type	Cause Of Issue	Type Of Loss	Country
Phishing attack	unsecured server	Data/Money	Missouri

Chinese Hacker Publishes PoC for Remote iOS 12 Jailbreak On iPhone X

Technical details of critical vulnerabilities in Apple Safari web browser and iOS were revealed by a Chinese cybersecurity researcher

Technical details of critical vulnerabilities in Apple Safari web browser and iOS were revealed by a Chinese cybersecurity researcher, which could possibly pave access for a remote attacker to jailbreak and compromise victims using iPhoneX running iOS 12.1.2 and before versions. To do so, all the attacker needs is to deceive iPhoneX users to open a crafted web page through the usage of Safari browser. Moreover, finding flaws and launching an exploit isn't simple for every iOS hacker. Qixun Zhao of Qihoo 360's Vulcan team was the first to discover this remote Jailbreak exploit, which is formed by the synthesis of two vulnerabilities, (CVE-2019-6227) in Apple and (CVE-2019-625) in iOS Kernel. The Safari flaw allows the malicious web content to run arbitrary code on the targeted device and then uses the second bug to ascend privileges and to install a malicious application, covertly. Nevertheless, the researcher decides not to publish the malicious code for iOS jailbreak in a bid to prevent malicious attacks against Apple Users. Hence, it is greatly advised for iPhone users to install the latest iOS updates without procrastination, instead of waiting for another jailbreak

Attack Type	Cause Of Issue	Type Of Loss	Country
malicious injection	Remote code execution	Dara/Money	China

TECHNOLOGY

Critical RCE Flaw in Linux APT Allows Remote Attackers to Hack Systems

cybersecurity experts on the sizzling topic, "Is HTTP's usage favourable (or) software's that only rely on signature based package verification favourable,

Argument between cybersecurity experts on the sizzling topic, "Is HTTP's usage favourable (or) software's that only rely on signature based package verification favourable, as APT on Linux does the same" has been brooding over twitter. Paradoxically, a security nerd exposed the details of a new critical remote code execution flaw in the apt-get utility which can be exploited by Man-In-The-Middle (MITM) attacks that are swift in compromising Linux machines. The error again proves if HTTPS is used for communication, such attacks can be alleviated easily. The vulnerability (CVE-2019-3462) was discovered by Max Justicz and it resides in APT package manager. It is a widely used utility that handles the installation, update and software removal on Debian, Ubuntu and on other Linux distributions. APT HTTP redirect helps Linux machines to automatically find compatible server for downloading software packages when others aren't available. If 1st server fails, it returns a response from the adjacent server, thus ensuring robustness. No software, platform or server can be tagged with the brand as "100% secure". Hence, adopting the ideology of a proactive approach towards security with defence-in-depth is always like a "welcoming a blessing". apt-get update is a part of various Linux distributions that comprises of Debian and Ubuntu. During mire situation, they acknowledge the flaws and release suitable security updates to fix the error. Hence, it is an undeniable indispensability for Linux users to update their systems without excuses.

Attack Type	Cause Of Issue	Type Of Loss	Country
Arbitrary attack	Remote code	Data	USA

Ukrainian Police Arrest 6 Hackers Linked to DDoS and Financial Attacks

Two distinctive group of hackers have been busted by the Ukrainian Police for launching DDoS attacks against news agencies and for stealing money from Ukrainian citizens

Two distinctive group of hackers have been busted by the Ukrainian Police for launching DDoS attacks against news agencies and for stealing money from Ukrainian citizens. The arrested two groups contained 4 hackers of 26-30 years whom stole more than 5 million Hryvnia (around 178,380 USD) from the accounts of Ukrainian citizens. The suspects executed their attacks by assessing vulnerable computers, corrupting them through Trojan malwares and using key-logging software technique on infected systems for capturing credentials. Once they gained access to financial data's, the perpetrators transferred the funds to their own accounts. Perhaps these, they have left a backdoor as a beneficiary for future plans execution. As per authorities, the duo developed a couple of DDoS tools which sends many automatic queries to targets, every second. The duo are facing the brunt of their retrospection deeds, by experiencing 6 years imprisonment under the article 361 of the Criminal Code of Ukraine.

Attack Type	Cause Of Issue	Type Of Loss	Country
DDos Attack	server flaw	Data/Money	Ukrain

FINANCE

Unprotected Government Server Exposes Years of FBI Investigations

Millions of sensitive government files of about 3 terabytes, belonging to the Oklahoma Department of Securities (ODS), were left exposed on an unsecured server over a week

Millions of sensitive government files of about 3 terabytes, belonging to the Oklahoma Department of Securities (ODS), were left exposed on an unsecured server over a week (found through Snoden). The unsecured server discovered by Greg Pollock, a researcher of cybersecurity firm 'UpGuard' also contained various decades worth of confidential case files, emails, social security numbers, names, addresses and list of PII (Personal Identifiable Information) with all open without password. Post the notification to ODS department by the UpGuard research team, the state agency removed the 'public access'. It is still hazy about the fact, "Has anyone else accessed it". If accessed in an unauthorized way, then the loss would be loathsome. The firm also detected that hackers remotely accessed the state agency's workstations, login information and passwords for several internet services as well as for a popular antivirus software. Regarding to this incident, Oklahoma Department of Securities said," a vulnerability was discovered and was rapidly secured in the server". Alongside this, the issue is taken seriously and a forensic investigation is also hired. The department is in a pursuit for remedial action of anyone's uncertainty over anyone's information, internal policies and security measures for ensuring the fortification of such incidents in future.

Attack Type	Cause Of Issue	Type Of Loss	Country
Injection attack	Unsecured Server	Data/Money	USA

Hackers infect e-commerce sites by compromising their advertising partner

Magecart 12- a new subgroup of Magecart, has struck again by compromising 277 e-commerce websites through supply-chain attacks

Magecart 12- a new subgroup of Magecart, has struck again by compromising 277 e-commerce websites through supply-chain attacks, reports security researchers. Magecart are a digital credit card skimmers whom launched attacks against gigantic firms like Ticketmaster, British Airways and Newegg. Magecart hackers compromise e-commerce sites and inflict dreadful JavaScript code that secretly seizes the payment data's of customers and then send it to the remote server. However, researchers from two firms revealed that Magecart group 12 hacked and infiltrated its skimming code into a 3rd party JavaScript library for enabling websites using that script to load malicious code. The targeted 3rd party library is a French online advertising company called as Adverline, whose service is used by many European e-commerce websites to display ads. Security researcher Yonathan Klijnsma at RiskIQ discovered that Magecart Group 12 shields from de-obfuscation and analysis by doing an integrity check on itself twice. If any of infected ones are detected, the script starts to carry out skimming behaviour by copying both from name and values. The pilfered data's are stored in JavaScript local storage under the key name `Cache' in Base64 format. Code generates a random number for specifying individual victims which then gets stored into local storage with key name E-tag.

Attack Type	Cause Of Issue	Type Of Loss	Country
supply chain attack	Firewall flaw	Data/Money	UK

TECHNOLOGY

Flight Booking System Flaw Affected Customers of 141 Airlines Worldwide

Half of the world flight travellers were exposed to a critical vulnerability in an online flight booking system

Half of the world flight travellers were exposed to a critical vulnerability in an online flight booking system which gave access for remote hackers to modify the users travel details and claim their frequent flyer miles. This vulnerability was discovered by an Israel network security researcher named as Noam Rotem, while booking a flight on Israeli airline ELAL, which needed just the victim's PNR (Passenger Name Record) number.

The traveller receives PNR number and a unique link after booking a flight with ELAL which allows the customers for finding their booking status and other information linked with PNR. Rotem revealed that by changing the value of "RULE_SOURCE_1_ID" parameter on that link to someone else PNR number can display the personal and booking-related data's associated with it. Rotem also revealed that Amadeus portal wasn't using any brute-force protection through which hackers can figure out all the active PNR numbers of customers linked with Amadeus airline website. As the Amadeus booking system is being used at least by 141 airlines, millions of travellers can be affected. After discovering the vulnerability, Rotem contacted ELAL and suggested airline defensive mechanisms to prevent against brute-force attempts. Post information, Amadeus has immediately fixed the issue. When contacted them, they said "Our technical teams took immediate action, and we can now confirm that the issue is solved."

Attack Type	Cause Of Issue	Type Of Loss	Country
Remote code attack	vulnerable attack	Data/Money	Globally

TECHNOLOGY

Fortnite Flaws Allowed Hackers to Takeover Gamers' Accounts

Check Point researchers discovered many security vulnerabilities in Fortnite

Check Point researchers discovered many security vulnerabilities in Fortnite (a familiar online game played by 80 million users), one of which allowed remote attackers to seize the player accounts by deceiving them to click a suspicious link. The reported Fortnite flaws comprised of SQL injection, cross-site scripting (XSS) bug, a web application firewall and an OAuth account takeover vulnerability. Players can log in to their game accounts using Single Sign-On (SSO) providers like Facebook, Google, Xbox and PlayStation accounts. According to researchers, combination of cross-site scripting (XSS) and malicious redirect issue allowed attackers to steal users authentication token by conjuring them to click on the link. Once data's are compromised, attacker can access data's and do whatever they want. One of the Epic Games had a SQL injection and a poorly-configured web application firewall vulnerability. If they were exploited, hackers would compromise it. Both Checkpoint and Epic Games, advise users to enable 2FA (two-factor authentication) for ensuring digital safety.

Attack Type	Cause Of Issue	Type Of Loss	Country
SQL Injection	firewall flaw	Data/money	ubiquitous

Unprotected VOIP Server Exposed Millions of SMS Messages, Call Logs

A California based Voice-Over-IP (VoIP) services provider has accidently left tens of gigabytes of customer data

A California based Voice-Over-IP (VoIP) services provider has accidently left tens of gigabytes of customer data that contains millions of call logs, SMS/MMS messages and plaintext internal system credentials which are publicly accessible by anyone without authentication. Justin Paine, the head of Trust and Safety at CloudFlare found an open ElasticSearch database last week using Shodan search engine. The database contained 6.7 million call logs on July 2017, 6 million SMS/MMS on December 2015 and 1 million logs containing API key. The call logs included timestamp and duration of VOIPO customers. The SMS and MMS included full content of messages. Apart from these, the exposed database had 1 million logs with many data's. These sensitive data's were exposed since 3rd June, 2018. The company of VOIPO said this was development server issue. Paine had an estimation that the leaked plaintext credentials were production based. The researcher also notified VOIPO about the unsecured ElasticSearch database on 8th January, 2019. The tragic truth is that, this isn't the 1st but 2nd time in this month where data exposure has been identified.

Attack Type	Cause Of Issue	Type Of Loss	Country
	unsecured server	Money	USA

TECHNOLOGY

36-Year-Old SCP Clients' Implementation Flaws Discovered

A set of 36 year-old vulnerabilities was uncovered in Secure Copy Protocol (SCP) implementation of various client applications.

A set of 36 year-old vulnerabilities was uncovered in Secure Copy Protocol (SCP) implementation of various client applications. Session Control Protocol (SCP) is a network protocol meant for users to transfer files securely between local host and a remote host using RCP (Remote Copy Protocol) and SSH protocol. It was discovered by Harry Sintonen, one of the F-Secure's senior Security Consultants saying that vulnerabilities exist due to improper validations. As per the advisory, many vulnerabilities were found in 2018 August which comprised of OpenSSH, Putty and WinSCP.

- SCP client improper directory name validation (CVE-2018-20685): A vulnerable SCP allows a remote SCP server to gain access and modify the contents.
- SCP client missing received object name validation (CVE-2019-6111): Allows harmful SCP server to overwrite arbitrary files in SCP directory.
- SCP client spoofing via object name (CVE-2019-6109): The client output can be tricked in progress display if missing character is encoded during progress display.
- SCP client spoofing via stderr (CVE-2019-6110): Allows infected server to alter the client output.

Since the vulnerabilities affect the implementation of SCP protocol, the files transferred through it are also affected. If you're worried of malicious SCP server, use SFTP (Secure FTP), for better safety.

Attack Type	Cause Of Issue	Type Of Loss	Country
spoofing attack	unsecured protocol	Data	USA

Unpatched vCard Flaw Could Let Attackers Hack Your Windows PCs

A zero day vulnerability, which makes a remote attacker to carry arbitrary codes on Windows machine was detected by and reported to Microsoft security team, by John Pag

A zero day vulnerability, which makes a remote attacker to carry arbitrary codes on Windows machine was detected by and reported to Microsoft security team, by John Page.
The vulnerability resides within the processing of a vCard file which is also braced by Microsoft Outlook. According to a researcher, a remote attacker can craft VCard file in zipped format or through drive-by-download techniques. Crafted data in a VCard file can causes Windows for displaying a hazardous hyperlink, researcher said. The user interface fails to give an indication of the hazard and hence, an attacker can use this vulnerability for executing code in the context of current user. The researcher who published the proof-of-concept exploit code has been assigned a CVSS 3.0 score of 7.8.

Attack Type	Cause Of Issue	Type Of Loss	Country
Remote attack	Lack of awareness	Data	Ubiquitous

Over 202 Million Chinese Job Seekers' Details Exposed On the Internet

Cybersecurity researcher discovered that more than 202 million citizen's records of 854.8 gigabytes were accessible to anyone on Internet,

Cybersecurity researcher discovered that more than 202 million citizen's records of 854.8 gigabytes were accessible to anyone on Internet, hosted by an American server hosting company. The compromised database included names, date of birth, phone number, email address, work experience and other personal stuff's. Bob Dianchenko, director of cyber risk research says that, "Someone could have used an old resume scraping tool called as 'data-import' for gleaning these jobseekers resumes, from Chinese websites like bj.58.com."

"Diachenko also communicated with BJ.58.com team who told that the leaked data didn't initiate from its website but from its 3rd party vendor.

"We have searched all over the database of us and investigated all the other storage, turned out that the sample data is not leaked from us," BJ.58.com confirmed Diache

Attack Type	Cause Of Issue	Type Of Loss	Country
phishing attack	Insecure mail server	Data/Money	China

New Systemd Privilege Escalation Flaws Affect Most Linux Distributions

Qualys researchers discovered 3 vulnerabilities CVE-2018-16864, CVE-2018-16865 and CVE-2018-16866 in Systemd.

Qualys researchers discovered 3 vulnerabilities CVE-2018-16864, CVE-2018-16865 and CVE-2018-16866 in Systemd. It is a familiar init system and service manager for most Linux operating systems that allows unprivileged local hackers to gain root access. However, some Linux distros like SUSE Linux Enterprise 15, openSUSE Leap 15.0 and Fedora 28 and 29 aren't affected as their user space is compiled with GCC's fstack cash protection. The 1st two flaws are memory rupture issues while the latter is capable of sensitive memory data exposure. To prevent these vulnerabilities from spearheading your Linux system, install the patches and be synchronized with updates, immediately upon their release.

Attack Type	Cause Of Issue	Type Of Loss	Country
privilege escalation	Lack Of awareness	Data	ubiquitous

Hackers Using Zero-Width Spaces to Bypass MS Office 365 Protection

Security researchers have warned people that cyber criminals and email scammers are being used to bypass security features of Microsoft office 365, including Safe links.

Security researchers have warned people that cyber criminals and email scammers are being used to bypass security features of Microsoft office 365, including Safe links. These Safe links are originally designed to protect users from malware and phishing attacks. They are included by Microsoft in Office 365 as an ATP (Advanced Threat Protection). Therefore, every time when users click on the link, Safe links first send them to Microsoft owned domain for checking suspicion. If Microsoft finds something malicious, it warns about it and if ain't, then it redirects to the original link. Researchers revealed that Safe Links URL protection features have been bypassed using Zero-Width-Spaces (ZWPs). Zero-Width-Spaces are non-printing Unicode characters such as:

- (Zero-Width Space)
- ‌ (Zero-Width Non-Joiner)
- ‍ (Zero-Width Joiner)

Attack Type	Cause Of Issue	Type Of Loss	Country
Malware &Phishing Attack	Lack of awareness	Data/Money	USA

TECHNOLOGY

Turns Out Kaspersky Labs Helped FBI Catch Alleged NSA Leaker

The news "The Shadow Brokers" and "The arrest of a NSA contractor convicted of stealing 50 Terabytes" are storming heavily throughout cosmos.

The news "The Shadow Brokers" and "The arrest of a NSA contractor convicted of stealing 50 Terabytes" are storming heavily throughout cosmos.
Kaspersky lab-The one banned in US government over human espionage fears is the one who tipped off the U.S government and helped FBI to catch NSA contractor T.Martin 111, post which the U.S government arrested him. The breach is believed to be the largest heist in America's history, far bigger than Edward Snowden.
Martin, who is about to go on trial in June, is currently facing 20 counts of unauthorized and wilful retention of national defence information. Ironically, Martin was arrested when FBI was engaged in an aggressive campaign against Kaspersky Labs in 2016. At the time of his arrest in August 2016, Martin worked for Booz Allen. It's the same company that exposed the secret surveillance programs carried out by NASA through Edward Snowden.

Attack Type	Cause Of Issue	Type Of Loss	Country
Malware	Server Flaw	Data	USA

Irish Tram Operator Website Hacked For Bitcoin Ransom

Dublin IRISH tram operator 'Luas' website is defaced after being targeted by hackers in a crave for bitcoin.

RANSOMWARE

Dublin IRISH tram operator 'Luas' website is defaced after being targeted by hackers in a crave for bitcoin. The hacker through a message claims to have breached security and to have publish "all data's" if ransom isn't paid within 5 days.

Luas in a statement has confirmed this morning that their "website is compromised and defaced". They also said that they will only use twitter for any travel updates in the meantime.

They further added that, "Please do not click on Luas website as it is down. We have technicians striving to resolve this issue as fast as possible. For any queries, dial our customer care number on 1850 300 604."

Attack Type	Cause Of Issue	Type Of Loss	Country
Ransomware	Lack Of awareness	Data	Iranland

Zero-Day Virus Forces EHR Downtime at 21 Health Science North Hospitals

Canada-based HSN at Sudbury discovered a virus infected its computer system; officials put its system on downtime to contain the exploit.

HEALTHCARE

On Thursday morning, staff at Canada-based HSN at Sudbury discovered a virus infected its computer system; officials put its system on downtime to contain the exploit.

On 18th January 2019, a zero day virus has disrupted the services of the computer system of Sudbury, of Ontario-based health sciences North. This forced officials to shut down its EHR to contain the infection, as per local news outlet CBC Radio-Canada.

"Zero day virus means it cannot be captured by anti-virus tools, available in market. All 24 hospitals in the region rely on our information technology platforms and to safeguard those sickbays, authorities implemented precautious measures like shutting down systems and more. Out of 24, 21 sickbays are functioning with main electronic health system" says Dominic Giroux, Health Sciences of North CEO.

"The virus didn't affect the cancer program system. We have good backup data to restore our lost information and so by Friday, we will restore most of our major systems for Health Sciences North."

Other hospitals also experienced care interruption with efficiency of services slowed down, Giroux explained.

Giroux insisted all non-urgent care needs to have a visit to clinic or to use a telehealth platform.

Attack Type	Cause Of Issue	Type Of Loss	Country
Virus Attack	Server Flaw	Data/Money	Canada

TECHNOLOGY

Scamvertisers using Botnets and Public Servers for Hire, Charged in New York

The United States Department of Justice has found a worthy reason to prosecute the alleged online scamvertising that involves eight Russian nationals

The United States Department of Justice has found a worthy reason to prosecute the alleged online scamvertising that involves eight Russian nationals. The scamvertising schemes were separately named as 3ve and Methbot that totally earns $36 in revenue for scamming and for generating Artificial traffic. Five most wanted suspects with hot pursuits from police are named as Boris Timokhin, Mikhail Andreev, Denis Avdeev, Dmitry Novikov and Aleksandr Isaev. Two more personalities from Kazakhstan are Yevgeniv Timchenko and Sergey Ovsyannikov. The Methobot and 3ve scamvertising projects have generated $7 million and $29 million income, respectively. The suspects are sued due to wire fraud, money laundering, aggravated identity theft, conspiracy to commit computer intrusion allegations and much more. The FBI is taking steps to excavate more truth from these culprits.

I thank and commend the U.S. Attorney for the Eastern District, and all the investigators with the FBI Cyber Division and the NYPD. Together, we are ensuring that the vital systems and technologies of our economy are kept safe," concluded James O'Neill, NYPD Commissioner.

Attack Type	Cause Of Issue	Type Of Loss	Country
Bots attack	lack of awareness	Money	USA

Attacks against Industrial Machines via Vulnerable Radio Remote Controllers: Security Analysis and Recommendations

Radio frequency (RF) remote controllers might look like your typical remote controllers:

Radio frequency (RF) remote controllers might look like your typical remote controllers: While some come in belt packs, most are pocket-sized and hand-held with buttons and joysticks. In principle, consumer and industrial radio remote controllers are very similar. Each device uses a transmitter (TX) that sends out radio waves corresponding to a command (or a button press), which a receiver (RX) interprets and reacts to, for example, lift a garage door open or lift a load via an overhead crane. The rugged and unassuming ones, however, come with heavy-duty purposes: control and automation of machines in various industrial sectors such as construction, manufacturing, logistics, and mining. And unlike the consumer-grade devices, industrial radio remote controllers are pervasively embedded in safety-critical applications.

Attack Type	Cause Of Issue	Type Of Loss	Country
Remote attack	Vulnerable server	Data/Money	USA

RANSOWARE

PyLocky Ransomware Decryption Tool Released — Unlock Files For Free

Security researcher Mike Bautista has released a free decryption tool that manumits victims infected by PyLocky ransomware attack, without paying ransom.

Security researcher Mike Bautista has released a free decryption tool that manumits victims infected by PyLocky ransomware attack, without paying ransom. The decryption tool works for everyone but with limitations. The initial network traffic (PCAP file) between PyLocky ransomware and its command-and-control (C2) server, must be captured which is generally done by none. Researchers at Trend Micro, first observed in July that PyLocky ransomware was manipulating through spam emails to trick victims. To prevent detection by sandbox security software, the ransomware torpers for 999.999 seconds if system size is less than 4 GB.
To be safe from these attacks:

- Beware of phishing emails
- Backup Regularly
- Maintain your Antivirus software and system up-to-date.

Attack Type	Cause Of Issue	Type Of Loss	Country
Ransomware	Lack Of awareness	Money/Data	USA

Life under GDPR: Data Breach Cost Unknown

What Impact Will European Privacy Rule Have on Class Action Lawsuits and Other Expenses?

What Impact Will European Privacy Rule Have on Class Action Lawsuits and Other Expenses?
EU's General Data Protection Regulation (GDPR), in effect from 25th May 2018 facilitates all EU protection officials the potentiality to impose intense penalties on firms that jeopardise to protect Europeans personal data carefully.
"Organizations are in a wait to check the repercussions that GDPR will have on breach landscape including the cost, companies face not just from clean up but also on class action lawsuits", says Thornton-Trump, head of cybersecurity at financial services firm AMTrust International, in London.
He concludes that, "What we infer from the occurrence of a data breach is that it's a painful experience on an organization. What we don't know is the fact that is the pain eternal or ephemeral."

Attack Type	Cause Of Issue	Type Of Loss	Country
GDPR attack	Vulnerable Firewall	Data	Europe

TECHNOLOGY

TECHNOLOGY

New Exploit Kit “Novidade” Found Targeting Home and SOHO Routers

A new exploit named as Novidade meaning `Novelty' in Portuguese, attacks the DNS (Domain name System) through Cross-Site Request Forgery (CSRF) with applications, the users are authenticated with. Novidade has been delivered through various techniques like malvertising, compromised website injection and via instant messengers. Once the victim clicks the link to Novidade and if the HTTP connection is successfully established, a corresponding exploit payload is executed, which is encoded Base64.

There are 3 variants of Novidade. They are:

- First Version: The basic variant of the exploit kit.
- Second Version: An advanced variant with JavaScript obfuscator that makes landing page look different.
- Third Version: The most advanced variant that retains the JavaScript obfuscator but refines the landing page. It also allows hacker to embed a shortened URL link.

Brazil was mostly affected by this attack and multiple compromised websites were being inflicted with an iframe, which redirected people to Novidade. To fortify from these exploit kits, users must upgrade their device firmware to newest version, must use strong passwords, should change router’s default IP address, disable remote access features and finally use HTTPS for secure connections.

Attack Type	Cause Of Issue	Type Of Loss	Country
CSRF attack	Insecure DNS	Data	USA

HEALTHCARE

Anonymous-affiliated hacker slapped with 10-year prison sentence for Boston Children's cyberattack

The federal judge in Boston who handed down the sentence called Gottesfeld a "self-aggrandizing menace."

Anonymous hacker Martin Gottesfeld was sentenced to more than 10 years along with $443,000 for perpetrating the damaging cyberattacks, declared the federal judge in Boston.

THE IMPACT:

The DDOS cyberattacks through Gottesfeld initiated from Massachusetts and then proliferated into a humongous extent on Boston Children’s hospital. Hence, the systems over there had to be shut down as their internet services which were meant to treat patients became crippled, says Reuters. The attacks initiated from Gottesfeld’s discern over a child custody about a Connecticut teenager Justin Pelletier.

ON THE RECORD

This was not a tens of thousands of dollars thing, it was significantly more than that," said Daniel Nigrin, commenting earlier to HFN on the financial ramifications of the cyberattack.

"It was your arrogance and misplaced pride that has been on display in this case from the very beginning that led you to believe you know more than the doctors at Boston Children's Hospital," U.S. District Judge Nathaniel Gorton said, according to the Boston Herald.

Attack Type	Cause Of Issue	Type Of Loss	Country
Cyber attack	Lack Of Awareness	Data	USA

TECHNOLOGY

Internet-of-Things (IoT) Security: Developments in VPN Filter and Emergence of Torii Botnet

FBI (Federal Bureau of Investigation) cautioned public of cyberattacks that affected over 500,000 routers in at least 54 countries,

Of late May, FBI (Federal Bureau of Investigation) cautioned public of cyberattacks that affected over 500,000 routers in at least 54 countries, compromising home and office routers. Fortunately, the FBI managed to sinkhole a domain/command-and-control (C&C) server that was used by VPNFilter. FBI found additional future attacks like:

- htpx: Redirects and inspects unencrypted traffic traversing through compromised devices.
- ndbr: Enables remote access to the device, turns it into a secure shell (SSH) client or server and transfers files via secure copy (SCP) protocol, which uses SSH.
- nm: Perform reconnaissance via a network-mapping and port-scanning tool; and search for certain routers to compromise.
- netfilter: Carries out denial of service by blocking IP addresses related to certain services and applications.
- portforwarding: Redirects traffic from the compromised device to an attacker-specified network.
- socks5proxy: Turns a compromised device into a virtual private network (VPN) server, which attackers then use as a ruse for network activity.
- tcpvpn: Enable remote access to internal networks compromised devices.

Attack Type	Cause Of Issue	Type Of Loss	Country
Bot attack	Unsecured Protocol	Data	USA

CONCLUSION

There is no 100% guarantee for security anywhere. So, main things to be safeguarded are the attack surfaces which needs to be secured against grotesque cyberattacks. For this, a proper security assessment from a dedicated and competent firm needs to be done mandatorily without fail, on a regular basis. Apart from this, proper awareness must be gained about all possible issues on cybersecurity. To know more, feel free to contact us anytime and we will help you for sure.

"A STITCH IN TIME SAVES NINE
HIRE US AND YOU'RE DATA'S WILL BE FINE."

REFERENCE LINKS

- https://cyware.com/news/abine-blur-password-manager-suffers-a-data-breach-exposing-private-data-of-24-million-users-6d165fdb
- https://cyware.com/news/kenyas-communication-authority-issues-an-alert-on-detection-of-emotet-trojan-07340896/
- https://cyware.com/news/blackmediagames-hacked-resulting-in-the-compromise-of-over-7-million-accounts-6135bd87
- https://cyware.com/news/security-researchers-report-the-latest-emotet-campaigns-propagation-technique-0b5d646b/
- https://thehackernews.com/2019/01/town-of-salem-data-breach.html
- https://thehackernews.com/2019/01/ethereum-double-spend-attack.html
- https://hackercombat.com/nasty-side-channel-attack-vulnerability-again-in-windows-linux-discovered/
- https://hackercombat.com/attacks-targeting-recent-php-framework-vulnerability-found/
- https://healthitsecurity.com/topic/latest-health-data-breaches
- https://healthitsecurity.com/news/months-long-phishing-attack-on-rehab-center-breaches-patient-data
- https://healthitsecurity.com/news/4-month-breach-of-benefitmall-impacts-112000-plan-members
- https://healthitsecurity.com/news/phishing-attack-hits-kent-county-community-mental-health
- https://healthitsecurity.com/news/third-party-vendor-phishing-attack-breaches-31000-patient-records
- https://healthitsecurity.com/news/ransomware-corrupts-24000-patient-records-of-california-specialist
- https://healthitsecurity.com/news/hackers-breach-data-of-4300-missouri-patients-for-3-months
- https://thehackernews.com/2019/01/ios12-jailbreak-exploit.html
- https://thehackernews.com/2019/01/linux-apt-http-hacking.html
- ttps://thehackernews.com/2019/01/php-pear-hacked.html
- https://thehackernews.com/2019/01/ukrainian-cybercriminals.html
- https://thehackernews.com/2019/01/oklahoma-fbi-data-leak.html
- https://thehackernews.com/2019/01/magecart-hacking-credit-cards.html
- https://thehackernews.com/2019/01/airlines-flight-hacking.html
- https://thehackernews.com/2019/01/fortnite-account-hacked.html
- https://thehackernews.com/2019/01/voip-service-database-hacking.html
- https://thehackernews.com/2019/01/web-hosting-server-security.html

- https://www.bankinfosecurity.in/blogs/data-breach-collection-contains-773-million-unique-emails-p-2713
- https://www.bankinfosecurity.in/insider-trading-sec-describes-41-million-hacking-scheme-a-11951
- https://www.healthcareitnews.com/news/ihis-and-singhealth-fined-s1-million-total-pdpc-data-breach-arising-cyberattack
- https://www.healthcarefinancenews.com/news/anonymous-affiliated-hacker-slapped-10-year-prison-sentence-boston-childrens-cyberattack
- https://healthitsecurity.com/news/trojan-malware-tops-ransomware-as-biggest-hacking-threat-to-healthcare
- https://healthitsecurity.com/news/zero-day-virus-forces-ehr-downtime-at-21-health-science-north-hospitals
- https://www.securitymagazine.com/articles/89645-healthcare-organizations-falling-behind-on-cyber-risk-management
- https://blog.trendmicro.com/trendlabs-security-intelligence/new-exploit-kit-novidade-found-targeting-home-and-soho-routers/
- https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/internet-of-things-iot-security-developments-in-vpnfilter-and-emergence-of-torii-botnet
- https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/attacks-against-industrial-machines-via-vulnerable-radio-remote-controllers-security-analysis-and-recommendations
- hps://thehackernews.com/2019/01/microsoft-windows-7-supprt.htmltt
- https://thehackernews.com/2019/01/scp-software-vulnerabilities.html
- https://thehackernews.com/2019/01/vcard-windows-hacking.html
- https://thehackernews.com/2019/01/ddos-attack-anonymous-hacker.html
- https://thehackernews.com/2019/01/pylocky-free-ransomware-decryption.html
- https://thehackernews.com/2019/01/mongodb-chinese-database.html
- https://thehackernews.com/2019/01/linux-systemd-exploit.html
- https://thehackernews.com/2019/01/phishing-zero-width-spaces.html
- https://thehackernews.com/2019/01/google-dns-over-tls-security.html
- https://thehackernews.com/2019/01/shadow-brokers-nsa-kaspersky.html
- ttps://hackercombat.com/dhs-issues-security-order-after-dns-hijack-attacks-from-iran/
- https://hackercombat.com/the-whatsapp-gold-scam-is-back-in-a-new-form/
- https://hackercombat.com/irish-tram-operator-website-hacked-for-bitcoin-ransom/
- https://www.bankinfosecurity.in/dharma-gang-pushes-phobos-crypto-locking-ransomware-a-11961
- https://www.bankinfosecurity.in/contactless-payments-new-wave-a-11960
- https://www.bankinfosecurity.in/interviews/life-under-gdpr-data-breach-cost-unknown-i-4226
- https://www.bankinfosecurity.in/hackers-wield-commoditized-tools-to-pop-west-african-banks-a-11957
- https://www.bankinfosecurity.in/facebook-deletes-more-bogus-accounts-linked-to-russia-a-11954
- https://www.bankinfosecurity.in/interviews/ransomware-pervasive-evolving-threat-i-4224

THREATSPLOIT ADVERSARY REPORT FEBRUARY 2019

www.briskinfosec.com