THREATSPLOIT

ADVERSARY REPORT

EDITION 35

BRISK INFOSEC
CYBER TRUST & ASSURANCE

www.briskinfosec.com

INTRODUCTION

Welcome to the Threatsploit Report of July 2021 covering some of the important cybersecurity events, incidents and exploits that occurred this month. This month, the cybersecurity sector witnessed a massive rise in ransomware and data breach attacks across geographies. Besides, many other attack types were seen spiking during these recent months.

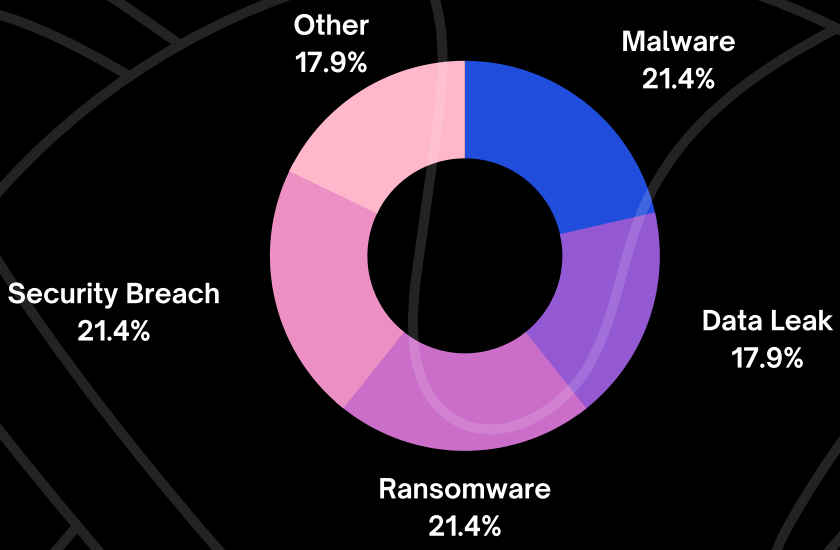
The primary reason is and has always been the same….

"Employees and stakeholders have limited or no perception or understanding of threats and misplaced understanding of massive cyber threats or consequences".

Since the time Work From Home (WFH) has become the new normal, security incidents has peaked with more and more issues relating to VPNs and other remote connecting mediums. WFH option has further limited the ability of IT functions to apply software patches for both old and new critical vulnerabilities, exposing the information assets for hackers to exploit and compromise. Let us walk you through some of the important security incidents that happened this month.

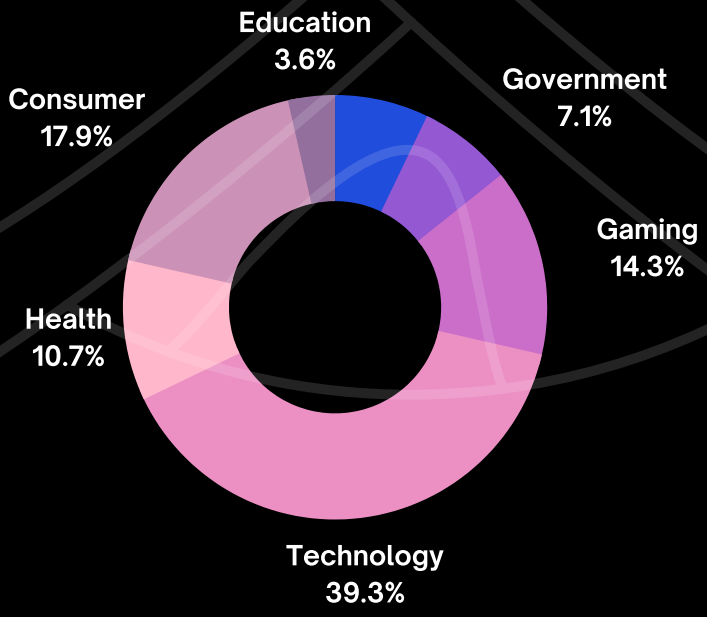
TYPES OF ATTACK VECTORS

The pie-chart indicates the percentage of malicious cyber-attacks that exploited the information infrastructure and compromised the security mechanisms across organisations from various business verticals.



SECTORS AFFECTED BY ATTACKS

The pie-chart indicates the percentage of malicious cyber-attacks that exploited the information infrastructure and compromised the security mechanisms across organisations from various business verticals.



LATEST THREAT ENTRIES

TECHNOLOGY

1. Fujifilm confirms ransomware attack on systems in Japan
2. 'Nameless' malware attacks 1.2TB database in the cloud
3. Facefish Backdoor delivers rootkits to Linux x64 systems
4. Google Researchers Discover A New Variant of Rowhammer Attack
5. DarkSide Pwned Colonial With Old VPN Password
6. Linux system service bug lets you get root on most modern distros
7. Hackers can exploit bugs in Samsung pre-installed apps to spy on users
8. Google fixes sixth Chrome zero-day exploited in the wild this year
9. Alibaba suffers billion-item data leak of usernames and mobile numbers
10. Wormable DarkRadiation Ransomware Targets Linux and Docker Instances
11. Cisco ASA vulnerability actively exploited after exploit released

HEALTH

1. Over a billion records belonging to CVS Health exposed online
2. Agent Tesla RAT Returns in COVID-19 Vax Phish
3. REvil STrikes Again – Ransomware Attack on UnitingCare Queensland

FINANCE

1. Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy
2. Spam Downpour Drips New IcedID Banking Trojan Variant

EDUCATION

1. New ChaChi Trojan Targeting U.S. Schools

GOVERNMENT

1. REvil ransomware hits US nuclear weapons contractor
2. Poland institutions and individuals targeted by an unprecedented series of cyber attacks

GAMING

1. EA: Gaming giant hacked and source code stolen
2. Cyberpunk 2077 Hacked Data Circulating Online
3. Steam Gaming Platform Hosting Malware
4. Battle for the Galaxy: 6 Million Gamers Hit by Data Leak

CONSUMER

1. Carnival discloses new data breach on email accounts
2. Audi, Volkswagen data breach affects 3.3 million customers
3. McDonald's discloses data breach after the theft of customer, employee info
4. Foodservice supplier Edward Don hit by a ransomware attack
5. Amazon Web Services Misconfiguration Exposes Half a Million Cosmetics Customers

TOOL OF THE DAY

1. SudoKiller
2. Paramspider
3. Tracy
4. PeePdf
5. Tidos Framework
6. h8mail

CYBER MONDAY

1. No one is immune to cyber attacks individuals or organisations of any size
2. Misconguration and acccout takeovers are the biggest cloud threats for every customers and vendors of the cloud
3. Cybersecurity is not an easy problem to solve for any business. Just when one challenge has been met, another variable appears

BLOG OF THE MONTH

1. Cloud Security And The Best Ways To Secure It From Breaches
2. Important Vulnerabilities And Smart Ways To Be Secured From Them
3. CRLF Injection Attack

CONSUMER TECH

Fujifilm confirms ransomware attack on systems in Japan

Fujifilm Corporation confirmed that the unauthorized access it became aware of in the late evening on June 1 was in fact a ransomware attack. In a statement, the company also said that the impact of the unauthorized access was confined to a specific network in Japan and that they had started to bring network, servers and computers confirmed as safe back into operation. Fujifilm said the company has been carrying out an investigation into the incident with a task force that included external experts and had reported the incident to the relevant government authorities and police.

Attack Type
Ransomware
Cause of Issue
Lack of Security
Type of Loss
Services
References
https://rb.gy/whl6oi

'Nameless' malware attacks 1.2TB database in the cloud

Attack Type
Malcious
Cause of Issue
Malware
Type of Loss
PII Data
References
https://rb.gy/ofujpi

Researchers on June 9th said a so-called "nameless" undetected malware stole a database in the cloud that contained some 1.2 terabytes of files, cookies, and credentials that came from 3.2 million Windows-based computers. NordLocker said the virus escaped with 6 million files that it grabbed from desktop and downloads folders. Screenshots made by the malware revealed that it spread via illegal Adobe PhotoShop software, Windows cracking tools, and pirated games. The malware also photographed the user if the device had a webcam.

Facefish Backdoor delivers rootkits to Linux x64 systems

Cybersecurity experts from Qihoo 360 NETLAB published details about a new backdoor, dubbed Facefish, which can be used by threat actors to steal login credentials and executing arbitrary commands on Linux systems. Juniper researchers also analysed the malware who observed the use of an exploit against the Control Web Panel (CWP) server administration web application to inject code via LD_PRELOAD and uses a custom, encrypted binary C2 to exfiltrate credentials and control the machines.

Attack Type
Rootkit Backdoor
Cause of Issue
Malware
Type of Loss
Unknown
References
https://rb.gy/ftbvfe

Google Researchers Discover A New Variant of Rowhammer Attack

A team of security researchers from Google has demonstrated yet another variant of the Rowhammer vulnerability that targets increasingly smaller DRAM chips to bypass all current mitigations, making it a persistent threat to chip security. Dubbed "Half-Double," the new hammering technique hinges on the weak coupling between two memory rows that are not immediately adjacent to each other but one row removed in an attempt to tamper with data stored in memory and attack a system.

Attack Type
Security Exploit
Cause of Issue
Unknown
Type of Loss
DRAM Data
References
https://rb.gy/3qmvza

DarkSide Pwned Colonial With Old VPN Password

Attack Type
Ransomware
Cause of Issue
Security Breach
Type of Loss
PII Data
References
https://rb.gy/i1wwpc

It took only one dusty, no-longer-used password for the DarkSide cybercriminals to breach the network of Colonial Pipeline Co. last month, resulting in a ransomware attack that caused significant disruption and remains under investigation by the U.S. government and cybersecurity experts. The news once again highlights the importance of password security, as it comes on the heels of a separate report that hackers leaked the largest password collection to date – a 100 gigabyte file called “RockYou2021” containing 8.4 billion passwords – on a popular hacker forum earlier this week.

Linux system service bug lets you get root on most modern distros

Unprivileged attackers can get a root shell by exploiting an authentication bypass vulnerability in the polkit auth system service installed by default on many modern Linux distributions. The polkit local privilege escalation bug (tracked as CVE-2021-3560) was publicly disclosed, and a fix was released on June 3, 2021. Even though many Linux distributions haven't shipped with the vulnerable polkit version until recently, any Linux system shipping with polkit 0.113 or later installed is exposed to attacks.

Attack Type
Authentication Bypass
Cause of Issue
Local Privilege CVE Bug
Type of Loss
Privileged Data
References
https://rb.gy/ftbvfe

Hackers can exploit bugs in Samsung pre-installed apps to spy on users

Attack Type
CVE Findings
Cause of Issue
Lack of Security
Type of Loss
Unknown
References
https://rb.gy/cjfbrc

Samsung is working on patching multiple vulnerabilities affecting its mobile devices that could be used for spying or to take full control of the system. The bugs are part of a larger set discovered and reported responsibly by one security researcher through the company’s bug bounty program. the hacker collected close to $30,000 since the start of the year, for disclosing 14 issues. The other three vulnerabilities are currently waiting to be patched. For seven of these already patched bugs, which brought $20,690 in bounties, Toshin provides technical details and proof-of-concept exploitation instructions in a blog post.

Google fixes sixth Chrome zero-day exploited in the wild this year

Google has released Chrome 91.0.4472.101 for Windows, Mac, and Linux to fix 14 security vulnerabilities, with one zero-day vulnerability exploited in the wild and tracked as CVE-2021-30551. Few details regarding the fixed zero-day vulnerability are currently available other than that it is a type confusion bug in V8, Google's open-source and C++ WebAssembly and JavaScript engine.

Attack Type
Software Vulnerability /Security Research
Cause of Issue
Zero-Day
Type of Loss
Unknown
References
https://rb.gy/wnozqm

Alibaba suffers billion-item data leak of usernames and mobile numbers

Attack Type
Data Leak
Cause of Issue
Security Breach
Type of Loss
PII Data
References
https://rb.gy/bdoaa5

Alibaba's Chinese shopping operation Taobao has suffered a data breach of over a billion data points including usernames and mobile phone numbers. The info was lifted from the site by a crawler developed by an affiliate marketer. Reports suggest that a developer created a crawler that was able to reach beneath information available to the human eye on Taobao. The crawler operated for several months before Alibaba noticed the effort.

Wormable DarkRadiation Ransomware Targets Linux and Docker Instances

Cybersecurity researchers are sounding the alarm bell over a new ransomware strain called "DarkRadiation" that's implemented entirely in Bash and targets Linux and Docker cloud containers, while banking on messaging service Telegram for command-and-control (C2) communications. "The ransomware is written in Bash script and targets Red Hat/CentOS and Debian Linux distributions," researchers from Trend Micro said in a report published last week. "The malware uses OpenSSL's AES algorithm with CBC mode to encrypt files in various directories. It also uses Telegram's API to send an infection status to the threat actor(s)." The findings come from an analysis of a collection of hacking tools hosted on the unidentified threat actor's infrastructure in a directory called "api_attack."

Attack Type
Ransomware
Cause of Issue
Security Breach
Type of Loss
Unknown
References
https://rb.gy/dqzblb

Cisco ASA vulnerability actively exploited after exploit released

Attack Type
Software Vulnerability /Security Research
Cause of Issue
Lack of Security Mechanisms
Type of Loss
Unknown
References
https://rb.gy/mqvw6x

Hackers are scanning for and actively exploiting a vulnerability in Cisco ASA devices after a PoC exploit was published on Twitter. This Cisco ASA vulnerability is cross-site scripting (XSS) vulnerability that is tracked as CVE-2020-3580. This vulnerability can allow an unauthenticated threat actor to send targeted phishing emails or malicious links to a user of a Cisco ASA device to execute JavaScript commands in the user's browser.

HEALTH

Over a billion records belonging to CVS Health exposed online

On Thursday, WebsitePlanet, together with researcher Jeremiah Fowler, revealed the discovery of an online database belonging to CVS Health. The database was not password-protected and had no form of authentication in place to prevent unauthorized entry. Upon examining the database, the team found over one billion records connected to the US healthcare and pharmaceutical giant, which owns brands including CVS Pharmacy and Aetna. The database, 204GB in size, contained event and configuration data including production records of visitor IDs, session IDs and more.

Attack Type
Data Leak
Cause of Issue
Security Breach
Type of Loss
Health Records
References
https://rb.gy/bdoaa5

Agent Tesla RAT Returns in COVID-19 Vax Phish

The Agent Tesla remote access trojan (RAT) is scurrying around the internet again, this time arriving via a phishing campaign that uses a COVID-19 vaccination schedule as a lure. Spotted by researchers at the Bitdefender Antispam Lab, the attackers are targeting Windows machines using emails with malicious attachments. The body of the mails take a business-email approach and ask recipients to review an "issue" with vaccination registration. In the current spate of attacks, the malicious attachment turns out to be a RTF document that exploits the known Microsoft Office vulnerability tracked as CVE-2017-11882, a remote code execution (RCE) bug stemming from improper memory handling. Once opened, the document downloads and executes Agent Tesla malware.

Attack Type
Trojan
Cause of Issue
Malware
Type of Loss
System Compromise
References
https://rb.gy/c5arxs

REvil STrikes Again – Ransomware Attack on UnitingCare Queensland

UnitingCare was a victim of malware called Sodinokibi/REvil which encrypted its files and attempted to delete backups. The attack shut down a range of UnitingCare's core systems and forced its facilities to revert to paper-based and manual workarounds to continue operating. It's been reported that the hospital and aged care facilities have now managed to bring most of its applications and systems back online. UnitingCare has confirmed that there was no evidence that any patient's health had been compromised by the cyber incident. UnitingCare is continuing to work with the Australian Cyber Security Centre and technical and forensic advisors to respond to the attack.

Attack Type
Ransomware
Cause of Issue
Security Breach
Type of Loss
Reputation
Data Loss
References
https://rb.gy/p5utm3

FINANCE

Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy

In a recent analysis, IBM security team found that an Ursnif (aka Gozi) banking Trojan variant is being used in the wild to target online banking users in Italy with mobile malware. Aside from the Ursnif infection on the victim's desktop, the malware tricks victims into fetching a mobile app from a fake Google Play page and infects their mobile device with the Cerberus Android malware. The Cerberus malware component of the attack is used by Ursnif's operators to receive two-factor authentication codes sent by banks to their users when account updates and money transfer transactions are being confirmed in real-time. Cerberus also possesses other features and can enable the attacker to obtain the lock-screen code and remotely control the device.

Attack Type
Trojan
Mobile Malware
Cause of Issue
Malware Apps
Type of Loss
System Compromise
References
https://rb.gy/dqzblb

Spam Downpour Drips New IcedID Banking Trojan Variant

The primarily IcedID-flavored banking trojan spam campaigns were coming in at a fever pitch: Spikes hit more than 100 detections a day. Researchers have seen a new variant of the IcedID banking trojan sliding in via two new spam campaigns. Written in English and carrying. ZIP files full of the malware – or links to such ZIP files – the new twist on the old banking trojan is a tweaked downloader, which the threat actors moved from the initial x86 version to the latest: an x86-64 version. They also ditched the fake command-and-control (C2s) servers that were found in the earlier configuration and which were likely there to complicate malware analysis, researchers said. Most of the payloads the researchers collected were IcedID (Trojan-Banker.Win32.IcedID), but they also came across a few samples of the Qbot banking trojan (Backdoor.Win32.Qbot, aka QakBot).

Attack Type
Trojan
Cause of Issue
Malware Files
Type of Loss
PII Data
References
https://rb.gy/ujhzfd

EDUCATION

New ChaChi Trojan Targeting U.S. Schools

BlackBerry Threat Research and Intelligence revealed that a new ChaChi Trojan is being used as a critical component in executing ransomware operations against U.S. schools. The new malware type is capable of performing traditional RAT actions such as data exfiltration, backdoor creation, and credential dumping from the Windows Local Security Authority Subsystem Service (LSASS). BlackBerry researchers believe the Trojan was created by cybercriminal group PYSA/Mespinoza, which has been active since 2018.

Attack Type
Trojan
Cause of Issue
Ransomware
Type of Loss
System Compromise
References
https://rb.gy/0yrwyz

GOVERNMENT

REvil ransomware hits US nuclear weapons contractor

US nuclear weapons contractor Sol Oriens has suffered a cyberattack allegedly at the hands of the REvil ransomware gang, which claims to be auctioning data stolen during the attack. The REvil ransomware operation listed companies whose data they were auctioning off to the highest bidder. As proof that they stole data during the attack, REvil published images of a hiring overview document, payroll documents, and a wages report. As a way to pressure Sol Oriens into paying the threat actor's extortion demands, the ransomware gang threatened to share "relevant documentation and data to other military agencies.

Attack Type
Ransomware
Cause of Issue
Lack of Security
Type of Loss
Data Loss
Reputation
References
https://rb.gy/r4zd2r

Poland institutions and individuals targeted by an unprecedented series of cyber attacks

Attack Type
Cyber-Attacks
Cause of Issue
Unknown
Type of Loss
Data Loss
References
https://rb.gy/xdqi0b

Last week, hackers breached the private email account of Michal Dworczyk, the head of the prime minister's office and member of the ruling Law and Justice party (PiS). The emails were later leaked through the instant messaging system Telegram. The media reported that the politicians targeted by the hackers used their private Gmail accounts for communications, instead of using their secure government accounts.

GAMING

EA: Gaming giant hacked and source code stolen

The attackers claimed to have downloaded source code for games such as FIFA 21 and for the proprietary Frostbite game engine used as the base for many other high-profile games. News of the hack was first reported by news site Vice, which said some 780GB of data was stolen.

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
Data
References
https://rb.gy/qv6dpd

Cyberpunk 2077 Hacked Data Circulating Online

Attack Type
Data Leak
Cause of Issue
Ransomware
Type of Loss
Data
References
https://rb.gy/g326lk

New data from the February hack of CD Projekt Red, the videogame-development company behind Cyberpunk 2077 and The Witcher series, is circulating online. Earlier this year, the company suffered a ransomware attack in which a cyberattack group "gained access to our internal network, collected certain data belonging to CD PROJEKT Capital Group and left a ransom note," the company said at the time. The ransomware also encrypted the company's systems, but CD Projekt Red was able to restore everything from backup – leaving the real issue to be the stolen data.

Steam Gaming Platform Hosting Malware

Look out for SteamHide, an emerging malware that disguises itself inside profile images on the gaming platform Steam, which researchers think is being developed for a wide-scale campaign. The Steam platform merely serves as a vehicle that hosts the malicious file, according to research from G Data: "The heavy lifting in the shape of downloading, unpacking and executing a malicious payload fetched by the loader is handled by an external component, which accesses the malicious profile image on one Steam profile. This external payload can be distributed via crafted emails to compromised websites.

Attack Type
Malware
Cause of Issue
Lack of Security
Type of Loss
Compromised Data
References
https://rb.gy/z30h70

Battle for the Galaxy: 6 Million Gamers Hit by Data Leak

Infosecurity has learned. AMT Games, which has produced a string of mobile and social titles with tens of millions of downloads between them, exposed 1.5TB of data via an Elasticsearch server. A research team at reviews site WizCase found the trove, which contained 5.9 million player profiles, two million transactions, and 587,000 feedback messages. Profiles typically feature player IDs, usernames, country, total money spent on the game, and Facebook, Apple or Google account data if the user linked these with their game account. The firm warned exposed users that their data might have been picked up by opportunistic cyber-criminals searching for misconfigured databases. Data on how much money individuals have spent on the site could enable fraudsters to target the biggest spenders, it added.

Attack Type
Data Leak
Cause of Issue
Lack of Security
Type of Loss
PII Data
References
https://rb.gy/xdqi0b

CONSUMER

Carnival discloses new data breach on email accounts

Carnival Corporation – which has been plagued by cyberattacks over the past few years – issued a breach disclosure on June 17th confirming hackers attacked email accounts and gained access to data about its customers and employees. The data accessed included names, addresses, phone numbers, passport numbers, dates of birth, health information, and, in some limited instances, additional personal information like social security or national identification numbers.According to Carnival, the impacted information includes "data routinely collected during the guest experience and travel booking process or through the course of employment or providing services to the company, including COVID or other safety testing."

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
PII Data
Reputation
References
https://rb.gy/3npsov

Audi, Volkswagen data breach affects 3.3 million customers

Audi and Volkswagen have suffered a data breach affecting 3.3 million customers after a vendor exposed unsecured data on the Internet.VWGoA states that the breach involved 3.3 million customers, with over 97% of those affected relating to Audi customers and interested buyers. The data exposed varies per customer but could range from contact information to more sensitive information such as social security numbers and loan numbers.

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
Data Loss
References
https://rb.gy/rbfllp

McDonald's discloses data breach after the theft of customer, employee info

Attack Type
Security Breach
Cause of Issue
Lack of Security
Type of Loss
Data Loss
Reputation
References
https://rb.gy/xcq2by

McDonald's, the largest fast-food chain globally, has disclosed a data breach after hackers breached its systems and stole information belonging to customers and employees from the US, South Korea, and Taiwan. The threat actors also stole personal information (including names, emails, phone numbers, and addresses) from customers in South Korea and Taiwan. However, the number of customer documents exposed in the incident was small, and the breach did not impact customers' payment info in any way.

Foodservice supplier Edward Don hit by a ransomware attack

New data from the February hack of CD Projekt Red, the videogame-development company behind Cyberpunk 2077 and The Witcher series, is circulating online. Earlier this year, the company suffered a ransomware attack in which a cyberattack group "gained access to our internal network, collected certain data belonging to CD PROJEKT Capital Group and left a ransom note," the company said at the time. The ransomware also encrypted the company's systems, but CD Projekt Red was able to restore everything from backup – leaving the real issue to be the stolen data.

Attack Type
Ransomware
Cause of Issue
Lack of Security
Type of Loss
Reputation
Data Loss
References
https://rb.gy/8werqm

Amazon Web Services Misconfiguration Exposes Half a Million Cosmetics Customers

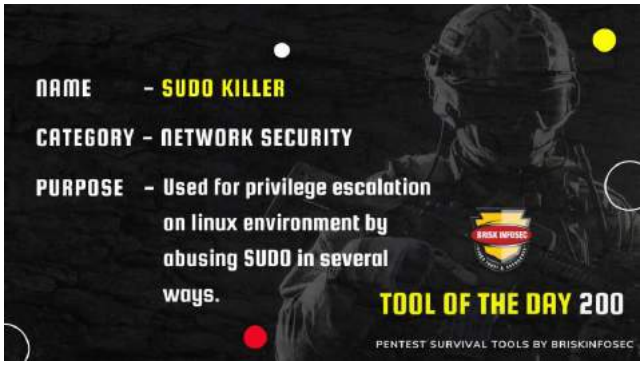
Attack Type
Data Leak
Cause of Issue
Lack of Security
Type of Loss
PII Data
References
https://rb.gy/jbb8oy

Hundreds of thousands of retail customers had their personal data exposed thanks to a misconfigured cloud storage account, Infosecurity has learned. A research team at reviews site WizCase traced the leaky Amazon S3 bucket to popular Turkish beauty products firm Cosmolog Kozmetik. The 20GB trove contained around 9500 files, including thousands of Excel files which exposed the personal information of 567,000 unique users who bought items from the provider across multiple e-commerce platforms.

TOOL OF THE DAY

SudoKIller

SUDO_KILLER is a tool that can be used for privilege escalation on a Linux environment by abusing SUDO in several ways. The tool helps to identify misconfiguration within sudo rules, vulnerability within the version of sudo being used (CVEs and vulns) and the use of dangerous binary, all of these could be abused to elevate privilege to ROOT.



ParamSpider

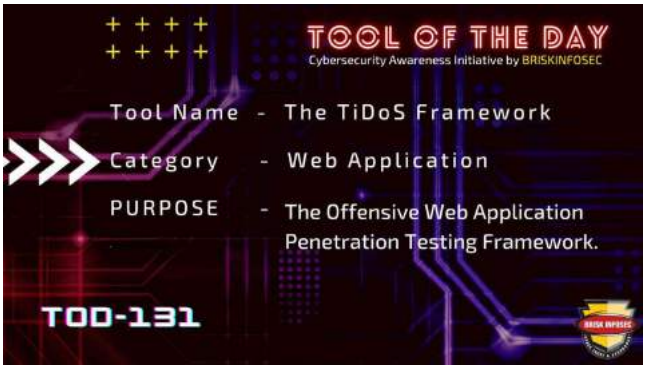
ParamSpider a parameter discovery suite.It finds parameters from web archives of the entered domain as well as from its subdomain without interacting the target host.It gives support to exclude urls with specific extensions.

Tracy

A pen-testing tool designed to assist with finding all sinks and sources of a web application and display these results in a digestible manner. Tracy should be used during the mapping-the-application phase of the pentest to identify sources of input and their corresponding outputs. Tracy can use this data to intelligently find vulnerable instances of XSS, especially with web applications that use lots of JavaScript.

PeePDF

peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks. With peepdf it's possible to see all the objects in the document showing the suspicious elements, supports all the most used filters and encodings, it can parse different versions of a file, object streams and encrypted files.



Tidos Framework

Tidos Framework is an open-source toolkit that performs all the major penetration testing tasks, such as reconnaissance,scanning, enumeration, and vulnerabilities analysis. All the tasks are performed in phases using the built-in modules. The total number of modules exceeds 100, with the majority used for reconnaissance and vulnerability analysis.

h8mail

h8mail is a tool for finding compromised email addresses and their passwords from these data breaches. When combined this tool with others such as TheHarvester or the crosslinked tool, you can harvest email addresses from an organization and then test to see if they have been compromised.

CYBER MONDAY

No one is immune to cyber attacks individuals or organisations of any size

Individuals and enterprises of all sizes, from small to large, have begun to establish an online presence. At this time, it is natural to conclude that cyber-attacks on any organization/individual are almost inevitable. To avert the very worst, the wisest choice to do is to maintain strict security measures for the sake of the business.

Misconfiguration and account takeovers are the biggest cloud threats for every customers and vendors of the cloud

Misconfigurations and account takeovers have become increasingly common in recent years. This is due to the fact that hackers have focused their attacks on mostly account takeover attacks. Hackers are also well-versed in how to approach a target differently due to weaknesses in typical configurations. As a result, companies must approach security from a variety of viewpoints.

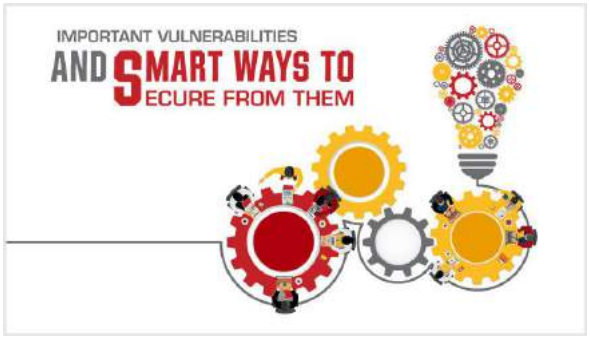
Cybersecurity is not an easy problem to solve for any business. Just when one challenge has been met, another variable appears

The majority of corporations are well aware of the shortcomings in the security procedures in place. Similarly, hackers are well aware of these issues and focus on chaining many medium level vulnerabilities in order to exploit a high/critical level vulnerability. It is nearly difficult to solve security concerns in a single attempt, however maintaining existing security measures can aid in the protection of one's digital assets.

BLOG OF THE MONTH

Cloud Security And The Best Ways To Secure It From Breaches

In this digital era, organizations are building their infrastructures and running their services in the cloud environment. When it comes to security, the danger is no stranger here due to its public accessibility. Over the recent years, the usage of cloud services had catapulted and plenty of information is being stored in the cloud environment. But parallelly, cloud-based cyberattacks have also increased.



Important Vulnerabilities And Smart Ways To Be Secured From Them

In Cybersecurity, despite a large number of new applications and advanced software, the number of vulnerabilities continues to increase. Security advancements are indeed stunning but fail to be on the winning side against security vulnerabilities, with the below facts testifying it.

CRLF Injection Attack

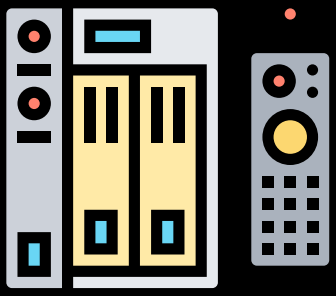
CRLF injection is carried out by an attacker by just simply inserting the carriage return line feed in the user input area to deceive the server or a web application, thus making them think that an object is terminated and another new object has been started. Reasons for CRLF injection: This vulnerability arises very commonly in the HTTP request of a web application that accepts the user-supplied input from an untrusted source, without being properly validated for malicious character (CRLF).

CONCLUSION

According to an article, online threats has risen by as much as six times their usual levels recently as the Covid 19 pandemic provided greater scope for cyber attacks. All the attacks mentioned above - their types, the financial and reputation impacts they have caused to organizations, the loopholes that paved way for such attacks invariably causing disaster to organizations - are just like a drop in an ocean. There are more unreported than that meets the eye. Millions of organizations and individuals have clicked those links and have fallen victims to these baits of hackers. The most obvious reason being 'lack of awareness. Well, as the saying goes,

"Prevention is better than Cure" - be it COVID-19 or Cyber threats.

Briskinfosec is ready to help you in your journey to protect your information infrastructure and assets. We assure you that we will help you to keep your data safe and also give you clear information on your company's current status and what are the steps needed to be taken to stay away from any kind of cyber attack.



contact@briskinfose.com | www.briskinfosec.com