MAY
2023

THREATSPLOIT ADVERSARY REPORT

EDITION 57

www.briskinfosec.com

Introduction :

The digital world is rapidly evolving, and with it, the threat landscape continues to expand. As technology advances, so do the techniques employed by cybercriminals to exploit vulnerabilities and compromise data. In this age of artificial intelligence, the challenges of cybersecurity have become even more complex. It is crucial for organizations to stay informed and proactive in mitigating these evolving threats.

> Security is not a product, but a process. It's about identifying and managing risks, staying one step ahead of potential threats, and continuously adapting to the ever-changing digital landscape."
>
> – Arulselvar Thomas, Director-Briskinfosec

Welcome to the Monthly Threatsploit Report for May 2023. This report aims to provide you with a comprehensive understanding of the latest cybersecurity incidents and threats that have emerged in the digital space. Our dedicated team at Briskinfosec has gathered information from various sources to keep you updated and help you strengthen your security posture.

Notable Attacks and Breaches :

1. Multinational ICICI Bank leaks passports and credit card numbers: The ICICI Bank suffered a data breach resulting in the exposure of sensitive customer information, including passports and credit card numbers.
2. American Bar Association data breach hits 1.4 million members: The American Bar Association experienced a significant data breach, impacting approximately 1.4 million members and potentially compromising their personal information.
3. Kubernetes RBAC Exploited in Large-Scale Campaign for Cryptocurrency Mining: Cybercriminals leveraged vulnerabilities in Kubernetes Role-Based Access Control (RBAC) to orchestrate a large-scale campaign for unauthorized cryptocurrency mining.

As the digital world continues to evolve, the importance of robust cybersecurity measures cannot be overstated. By staying informed about the latest threats and implementing proactive security practices, organizations can effectively mitigate risks and protect their valuable data assets. We encourage you to review the complete Threatsploit report for a detailed analysis of each incident and recommended strategies for enhancing your cybersecurity defenses.

Remember, cybersecurity is a journey, and we are here to support you every step of the way. Together, we can navigate the ever-changing digital landscape and ensure a secure future for your organization.

Best regards,
Briskinfosec Threat Intelligence Team

Contents :

Multinational ICICI Bank leaks passports and credit card numbers

The Indian government designated the ICICI Bank's resources as "critical information infrastructure" in 2022, implying that any damage to them might compromise national security. Despite the poor state of bank infrastructure on a national scale, the security of essential data was not secured. The Cybernews investigative team determined that the bank disclosed the sensitive data due to a misconfiguration of its systems during the current investigation.Because financial services are a popular target for cybercriminals, if bad actors gained access to the exposed data, the organisation might have faced severe consequences and put customers at danger. The Cybernews research team discovered a misconfigured and publicly available cloud storage - Digital Ocean bucket - with over 3.6 million ICICI Bank data on February 1. The files exposed important data about the bank and its customers.It included bank account details, credit card numbers, full names, dates of birth, home addresses, phone numbers, and emails among the exposed client data. The bucket also contained files with client passports, IDs, and Indian PANs - Indian taxpayer identity numbers. Bank statements and completed know-your-customer (KYC) forms were also made public. Another threat is data being sold on the dark web, as well as ICICI Bank becoming a target of ransomware attacks.

Phising Attack

Misconfiguration of their system

Banking Sector

American Bar Association data breach hits 1.4 million members

Hackers accessed the American Bar Association's (ABA) network and acquired access to older credentials for 1,466,000 members, resulting in a data breach. On March 17th, 2023, the ABA began notifying members that a hacker had been identified on its network and may have gotten access to members' login credentials for a legacy member system deactivated in 2018.The ABA noticed unusual activity on their network on March 17, 2023. "The incident response plan was activated immediately, and cybersecurity experts were retained to assist with the investigation," says a notice email issued to impacted subscribers and obtained by BleepingComputer. On March 23, 2023, an unauthorised third party obtained usernames and hashed and salted passwords that you may have used to access online accounts on the previous ABA website before to 2018 or the ABA Career Centre since 2018. The ABA informed BleepingComputer that this breach affected 1,466,000 members. They were instead hashed and salted, which is a procedure that adds random characters to the plain text password, which is subsequently turned into cybertext on the ABA systems. All ABA members should be on the lookout for spear-phishing emails imitating the ABA, since threat actors may use them to get further personal information.

Data breached

Hackers compromised its network

Government and Public Sector

Kubernetes RBAC Exploited in Large-Scale Campaign for Cryptocurrency Mining

A large-scale attack campaign uncovered in the wild has been creating backdoors and running bitcoin miners using Kubernetes (K8s) Role-Based Access Control (RBAC). The attackers also used DaemonSets to take over and syphon resources from the K8s clusters they targeted, according to a report supplied with The Hacker News by cloud security firm Aqua. The Israeli firm, which dubbed the attack RBAC Buster, said it discovered 60 vulnerable K8s clusters that were exploited by the threat actor behind the operation. The attacker gained early access through a misconfigured API server, then checked for indications of competing miner software on the compromised server, and finally used RBAC to set up persistence. Interestingly, some of the strategies detailed in the campaign are similar to those used by another illegal cryptocurrency mining business that used Daemon Sets to mint Dero and Monero. It is yet unknown whether the two sets of attacks are linked.

Cryptocurrency miners

Misconfigured API server

IT industry

Legion : A Python-Based Hacking Tool Targets Websites and Web Services

Legion, a Python-based credential harvester, is touted as a tool for threat actors to exploit numerous online services. This hacking tool is related to another malware family known as AndroxGh0st, although the identified sample has not been detected by any antivirus engines on VirusTotal.According to Cado Labs, the primary purpose of Legion is to allow attackers to hijack services and weaponize infrastructure for future assaults such as mass spam and phishing.Legion steals AWS credentials from misconfigured web servers and sends SMS spam to Sprint, T-Mobile, AT&T, Virgin, and Verizon customers.Legion relies mainly on misconfigurations in online services, therefore users should check their existing security protocols and verify secrets are properly maintained. Furthermore, AWS users should be aware of such programmes targeting IAM and SES services and should take proper security precautions.

Phishing and spam attacks

Misconfigured web servers

Cybersecurity industry

GhostToken Flaw Could Let Attackers Hide Malicious Apps in Google Cloud Platform

Details of a now-patched zero-day issue in Google Cloud Platform (GCP) that might have allowed threat actors to hide an unremovable, malicious application inside a victim's Google account have been revealed by cybersecurity experts.The issue, dubbed GhostToken by Israeli cybersecurity firm Astrix Security, affects all Google accounts, including enterprise-focused Workspace accounts. On June 19, 2022, it was discovered and reported to Google. On April 7, 2023, the business released a global patch after more than nine months.

Ghost Token flaw

Misconfigured web servers

IT industry

" Furniture rental startup RentoMojo reports data breach by hackers, 1.5 lakh subscribers to be affected "

RentoMojo notified its members via email that the company has discovered a security compromise, writing, recently, our team identified a security breach that involved unauthorised access to one of our databases. It appears that the attackers gained unauthorised access to our customer data, including personally identifiable information in certain circumstances, by exploiting the cloud misconfiguration via exceptionally sophisticated attacks, thereby penetrating one of our databases. The company also stated that the breach will have no effect on any financial information such as credit cards, debit cards, or UPI because they are never stored in the company's database.

Cyber attack

Misconfigured Databases

Rental industry

ChatGPT Account Takeover Bug Allows Hackers To Gain User's Online Account

"An independent security expert recently identified an important security vulnerability in ChatGPT that allows attackers to quickly exploit the vulnerability and take complete control of any ChatGPT user's account.The attacker can trick a web server into maintaining a web cache by providing a non-existent URL with a non-existent file type such as CSS, JPG, or PNG.This non-existent URL is distributed to victims through private or public chat rooms, where victims frequently click. The attacker visits this URL, which provides various critical bits of information."

Web Cache Deception

Manipulation of Server

AI Platform

Volvo retailer leaks sensitive files

"The Cybernews investigative team discovered that Dimas Volvo, a Volvo automobile store in Brazil, has been leaking sensitive material through its website for nearly a year. The revealed files may have been used by bad actors to hijack the official channels of communication and infiltrate the company's networks, among other things. Volvo's retailer revealed authentication details for its databases, including MySQL and Redis database hosts, open ports, and credentials. These credentials might then be used to get access to the databases' contents, which could contain private user data. Researchers also discovered the Laravel application key for the website. This key's vulnerability is especially risky because it might have been used to decrypt user cookies, which frequently contain sensitive information such as credentials or session IDs. An attacker could use this information to get access to the victim's account. Researchers detected the URL of the Git repository where the website's source code is stored among the exposed data, revealing the file's name and who created it.

Because guessing a password is faster than guessing a username and password, attackers may have used leaked credentials to brute force access to the repository.Attackers might have used the website's structure information to determine the technologies used in its development and streamline a long variety of approaches to potentially attack the website."

Cybersecurity breach

Risk of breached comms

Automobile Industry

Hyundai data breach exposes owner details in France and Italy

"Hyundai disclosed a data breach affecting Italian and French car owners, as well as those who scheduled a test drive, and has warned that hackers obtained access to personal information. The letter also states that the hacker who gained access to Hyundai's database did not steal financial or identification information. Hyundai claims that in reaction to the issue, they recruited IT professionals, who have taken the impacted systems down until additional security measures are applied. In the same email, the South Korean automaker urges customers to be cautious of unsolicited e-mails and SMS texts that claim to come from them, since they may be phishing or social engineering attempts. Although there is no evidence that the data in disputing has been used for fraudulent purposes, we urge you to exercise extreme caution and verify any contact attempt via e-mail, mail, and/or text message that appears to come from Hyundai Italia or other entities of the Hyundai Group. In February 2023, the business released emergency software upgrades for various car models that had been compromised by a simple USB cable hack that allowed thieves to steal them. Bugs in the Hyundai app allowed remote attackers to unlock and start certain afflicted vehicles in December 2022, as well as leak car owner information."

Phishing and social engineering attempts

USB cable hack

Automobile Industry

Hacked sites caught spreading malware via fake Chrome updates

Hackers compromise websites in order to inject scripts that display fake Google Chrome automatic update issues, distributing malware to innocent visitors.The attack begins by infiltrating websites in order to inject malicious JavaScript code that executes scripts when users visit them. Depending on whether the visitor is part of the intended audience, these scripts will download additional scripts.These malicious scripts are distributed via the Pinata IPFS (InterPlanetary File System) service, which hides the origin server hosting the files, rendering blocklisting useless and resisting takedowns.When a targeted visitor visits the site, the scripts will display a fake Google Chrome error page indicating that an automated update required to continue observing the site failed to install.The scripts will then download a ZIP file called'release.zip' that appears as a Chrome update that the user should install.When this malware is launched, it transfers itself to C:Program FilesGoogleChrome as "updater.exe" and then starts a legal programme to execute process injection and run directly from memory.It disables Windows Update and interferes with security products' connectivity with their servers by changing the IP addresses of the latter in the HOSTS file. This restricts updates and threat detection, and may even stop an antivirus entirely.Always install security updates for installed software from the product's makers or through automatic updates integrated into the programme, rather than through third-party sites.

BYOVD

Manipulation of Server

IT industry

Kodi discloses data breach after forum database for sale online

The Kodi Foundation has announced a data breach after hackers stole and attempted to sell the organization's MyBB forum database, which contained user data and private messages. Hackers taken the forum database by getting into the Admin console with the credentials of an inactive staff member. They created and downloaded database backups many times in 2023 after gaining access to the admin panel.The account was used to generate backups of databases, which were then downloaded and erased. It also downloaded the database's existing nightly full backups.The Kodi team acknowledged that the actual account owner did not carry out these operations on the admin console, indicating that the staff member's credentials were most likely stolen.All public forum posts, staff forum posts, private messages communicated between users, and forum member data, including usernames, email addresses, and encrypted (hashed and salted) passwords produced by the MyBB (v1.8.27) software, are included in the stolen database. Considering the fact that the passwords were hashed and salted, Kodi warns that all credentials should now be regarded as breached. The administration team is planning a global password reset, which is certain to have an impact on service availability. Finally, once everything is back up and running, the Kodi team intends to conduct vulnerability tests. They are looking for competent auditors who are willing to offer their time and expertise to assist them with this cybersecurity effort.

Data breached

Risk of breached comms

Software Industry

KFC, Pizza Hut owner discloses data breach after ransomware attack

"The Cybernews investigative team discovered that Dimas Volvo, a Volvo automobile store in Brazil, has been leaking sensitive material through its website for nearly a year. The revealed files may have been used by bad actors to hijack the official channels of communication and infiltrate the company's networks, among other things. Volvo's retailer revealed authentication details for its databases, including MySQL and Redis database hosts, open ports, and credentials. These credentials might then be used to get access to the databases' contents, which could contain private user data. Researchers also discovered the Laravel application key for the website. This key's vulnerability is especially risky because it might have been used to decrypt user cookies, which frequently contain sensitive information such as credentials or session IDs. An attacker could use this information to get access to the victim's account. Researchers detected the URL of the Git repository where the website's source code is stored among the exposed data, revealing the file's name and who created it.

Ransomware Attack

Misconfigured web servers

Food industry

Samsung employees unwittingly leaked company secret data by using ChatGPT

Employees at Samsung have exchanged internal papers with the popular chatbot service ChatGPT, including meeting notes and source code. Samsung engineers utilised ChatGPT to evaluate the company's source code, instructing the chatbot to optimise test sequences for detecting flaws in the semiconductors they were building. According to the website Techradar, the corporation suffered three data leaks in less than a month as a result of its employees disclosing important information using ChatGPT. According to the release, there is no legal basis for the platform's enormous gathering and use of personal data to 'train' the algorithms on which it is based.

Data leakage

Misconfigured web servers

Communication industry

MSI hit in cyberattack, warns against installing knock-off firmware

MSI-brand motherboards, GPUs, laptops, PCs, and other equipment owners should take caution when updating their device's firmware or BIOS after the manufacturer disclosed a recent attacked.MSI advised customers to "obtain firmware/BIOS updates only from its official website," and not to utilise files obtained from other sources. MSI made no mention of the scope of the security breach or what was stolen, instead noting that it "detected network anomalies" and that its IT department "activated relevant defence mechanisms and carried out recovery measures."It further minimised any potential consequences, noting that it had resumed normal operations and did not expect any "significant impact" on its financials. However, it is unclear whether consumer data was exposed in the network attack at this time. MSI made no mention of the scope of the security breach or what was stolen, instead noting that it "detected network anomalies" and that its IT department "activated relevant defence mechanisms and carried out recovery measures."

Supply chain attack

Malicious SIte

IT industry

16,000 school documents have been leaked on the dark web

"Hackers posted 16,000 Tasmanian education department papers on the dark web, including personal information about schoolchildren.Madeleine Ogilvie, Minister of Science and Technology, stated that thousands of financial statements and invoices containing the names and addresses of school kids and their parents had been published after the third-party file transfer service GoAnywhere MFT was hacked.This data was obtained via a third-party file transfer service, and as previously stated, there is no evidence that Tasmanian government IT systems were compromised.He stated that the hackers had not made any ransom demands, but the federal authorities advised not to pay a ransom if one was given."

Data breached

Misconfigured web servers

Education industry

Database Snafu Leaks 600K Records from Marketplace

"According to vpnMentor, a data leak exposed hundreds of thousands of private details on an internet marketplace where people exchange cheap online accounts, licence keys, and malware.Jeremiah Fowler, a security researcher, found 600,000 ""customer support attachments"" associated to the website Z2U, which comprised photographs of people holding credit cards, passports, and other identification documents. Payment transactions, including IBAN numbers, user account logins, emails, and passwords, and order confirmations revealing the buyer's name, email, and purchase information were also exposed in the non-password secured database."

Data breached

Misconfiguration of database

Marketing Industry

Uber driver info stolen yet again : This time from law firm

More of Uber's internal data has been taken from a third party that experienced a security breach. Miscreants stole the personal information of the app's drivers from the IT systems of legal firm Genova Damage this time.Uber has not answer to The Register's inquiry regarding how many of its drivers' records were stolen.They determined that between January 23, 2023 and January 31, 2023, an unauthorised third party got access to our systems and certain limited files were accessed or exfiltrated.Following the investigation, the attorneys notified law enforcement, changed all system passwords, and agreed to take "additional steps to improve security and better help protect against similar incidents in the future."This occurred last year, after a separate third-party hack. A cyber criminal calling themselves UberLeaks broke into the network of software vendor and Uber supplier Teqtivity and posted data belonging to Uber employees on BreachForums.Although no Uber consumer data was compromised, information on over 77,000 Uber and UberEats employees was released. Some of the information revealed was also on third-party vendor services and mobile device management systems used by Uber.

Supply chain attack

Unauthorized access to its databases

Transportation industry

Service NSW breach exposes personal data affecting thousands of customers

During a privacy incident, the personal information of Service NSW customers was exposed to other logged-in persons.The data breach was caused by a March 20 upgrade to the "My Services" dashboard. Driver's licence and vehicle registration details, contact information, and children's names were among the personal information available through linked services that may have been visible. The number of customers affected by the incident is unknown.Service NSW has stated that it is examining the extent of the problem, and that the Information and Privacy Commission, as well as concerned customers, have been contacted. According to a Service NSW spokesman, about 3700 consumers may have been disrupted by the event. The NSW government committed $315 million in cyber systems last November, introduced the Privacy and Personal Information Protection Amendment Bill, and formed ID Support NSW to assist those affected by identity theft.

Privacy Breach

Misconfiguration of their system

Government executive agency

500k Impacted by Data Breach at Debt Buyer NCB

NCB Management Services, a national accounts receivable management company and debt buyer, has begun notifying about 500,000 people that their personal information was exposed in a data breach. On February 1, an unauthorised entity breached certain of NCB's systems and acquired access to Bank of America credit card account information, according to NCB. On February 4, the problem was identified, and the data theft was confirmed on March 8. According to the organisation, exposed personal information includes names, addresses, phone numbers, email addresses, birth dates, driver's licence numbers, Social Security numbers, and employment positions. Pay amounts, credit card numbers, routing numbers, account numbers and balances, and/or account statuses were also stolen. The impacted credit card accounts, according to NCB, had already been closed when the cyberattack happened. The event did not involve a breach of Bank of America's systems. The corporation also claims that it is unclear of potentially accessed information being distributed or maliciously exploited. Unauthorised activity on NCB's systems has ceased, and NCB has received assurances that the third party no longer has access to any of the information on its systems.

Data breached

Compromising of NCB's systems

BPO Services

Over a Million Financial Records Exposed in Data Incident Involving Fintech Company

Invoices from both individuals and businesses who utilised an app to pay for items and services were included in the PDF documents made public. Names, email addresses, physical addresses, phone numbers, and other information were included on the bills. Furthermore, the paperwork included comments on what the payment was for, the total amount, the due date, and some even included tax information such as a tax id number.The information was discovered to belong to NorthOne Bank, a financial technology company used by over 320,000 American businesses.Anyone with an internet connection and the database's URL could see or download the.Documents in PDF format. There were minimal security procedures in place to prevent a complete indexing of all papers. I guessed that there were over a million files marked as "production" in the database. In a random sample of 1,000 invoices, I saw billing amounts ranging from $60 to more than $10,000 for various services. Home repairs, pet services, food and drinks, and even medical care were among them.

Privacy Breach

Non-password protected database

Financial Industry

Sudan hackers target top hospitals in Hyderabad, slow down systems

Invoices from both individuals and businesses who utilised an app to pay for items and services were included in the PDF documents made public. Names, email addresses, physical addresses, phone numbers, and other information were included on the bills. Furthermore, the paperwork included comments on what the payment was for, the total amount, the due date, and some even included tax information such as a tax id number.The information was discovered to belong to NorthOne Bank, a financial technology company used by over 320,000 American businesses.Anyone with an internet connection and the database's URL could see or download the.Documents in PDF format. There were minimal security procedures in place to prevent a complete indexing of all papers. I guessed that there were over a million files marked as "production" in the database. In a random sample of 1,000 invoices, I saw billing amounts ranging from $60 to more than $10,000 for various services. Home repairs, pet services, food and drinks, and even medical care were among them.

DDoS attack

Compromises privacy of patients

Healthcare industry

Sensitive NATO Data Leaked After Cyber Attack On Portugal's Armed Forces

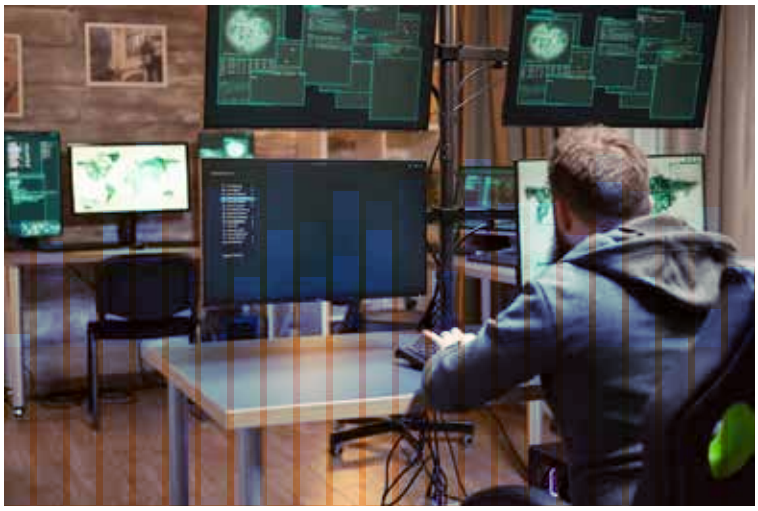
"On September 8th, the local Portuguese news organisation Diario de Noticias stated that the Portuguese Government Department of Defence was the victim of a major data breach including the leakage of important NATO papers that were published and sold on the dark web. Following an inquiry, it was discovered that unsecure channels were used for data transmission. The data exfiltration attack was built in such a way that it was undetectable, and it was conducted through a bot network that was particularly geared to collect sensitive data.

The department that suffered the breach is suspected of violating protocol, which resulted in the incident. They also concluded that the attack was built in such a way that it was undetectable, and that it was conducted using a computerised network designed mainly to acquire sensitive data."

Data breached

Unsecure channels were used for transmission of data

Intergovernmental military alliance



"Ferrari hit by ransomware, hackers leak 7 GB of data"

A file from Ferrari's website was leaked on a dark web leak site run by the ransomware group RansomEXX. Hackers claim to have gotten internal documents, datasheets, repair manuals, and other sensitive material.The stolen data set is over 7 GB in size. A snapshot of the leaked material depicts a document labelled 'confidential.' It appears to be a purchase agreement for a certain model of a Ferrari automobile. The disclosure is the second time in less than a year that Ferrari's data have been stolen by hackers. The Italian manufacturing company Speroni was targeted by the Everest cyber gang in December 2021. Threat actors promoted stealing 900 GB of data from Speroni, which contained critical information about the company's partners, including Ferrari, Lamborghini, Fiat Group, and other Italian automakers. Threat actors disrupted Ferrari's launch into the NFT market earlier this year. Almost immediately after Ferrari announced that it will mint tokens based on Ferrari automobiles, threat actors took over the company's subdomain and used it to host an NFT scam. Surprisingly, RansomEXX released the information less than a week after Bitdefender, a Romanian cybersecurity firm, became an official sponsor of Ferrari's Formula One (F1) racing team.

Ransomware Attack

Unauthorized access of database

Automobile Industry

Kubernetes RBAC Exploited in Large-Scale Campaign for Cryptocurrency Mining

A large-scale attack campaign uncovered in the wild has been creating backdoors and running bitcoin miners using Kubernetes (K8s) Role-Based Access Control (RBAC). The attackers also used DaemonSets to take over and syphon resources from the K8s clusters they targeted, according to a report supplied with The Hacker News by cloud security firm Aqua. The Israeli firm, which dubbed the attack RBAC Buster, said it discovered 60 vulnerable K8s clusters that were exploited by the threat actor behind the operation. The attacker gained early access through a misconfigured API server, then checked for indications of competing miner software on the compromised server, and finally used RBAC to set up persistence. Interestingly, some of the strategies detailed in the campaign are similar to those used by another illegal cryptocurrency mining business that used DaemonSets to mint Dero and Monero. It is yet unknown whether the two sets of attacks are linked.

Cryptocurrency miners

Misconfigured API server

IT industry

Legion : A Python-Based Hacking Tool Targets Websites and Web Services

Legion, a Python-based credential harvester, is touted as a tool for threat actors to exploit numerous online services. This hacking tool is related to another malware family known as AndroxGh0st, although the identified sample has not been detected by any antivirus engines on VirusTotal. According to Cado Labs, the primary purpose of Legion is to allow attackers to hijack services and weaponize infrastructure for future assaults such as mass spam and phishing. Legion steals AWS credentials from misconfigured web servers and sends SMS spam to Sprint, T-Mobile, AT&T, Virgin, and Verizon customers.Legion relies mainly on misconfigurations in online services, therefore users should check their existing security protocols and verify secrets are properly maintained. Furthermore, AWS users should be aware of such programmes targeting IAM and SES services and should take proper security precautions.

Phishing and spam attacks

Misconfigured web servers

Cybersecurity industry

GhostToken Flaw Could Let Attackers Hide Malicious Apps in Google Cloud Platform

Details of a now-patched zero-day issue in Google Cloud Platform (GCP) that might have allowed threat actors to hide an unremovable, malicious application inside a victim's Google account have been revealed by cybersecurity experts.The issue, dubbed GhostToken by Israeli cybersecurity firm Astrix Security, affects all Google accounts, including enterprise-focused Workspace accounts. On June 19, 2022, it was discovered and reported to Google. On April 7, 2023, the business released a global patch after more than nine months.

Ghost Token flaw

Misconfigured web servers

IT industry

CORPORATE OFFICE

Briskinfosec Technology and Consulting Pvt ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.
+91 86086 34123 | 044 4352 4537

contact@briskinfosec.com
www.briskinfosec.com