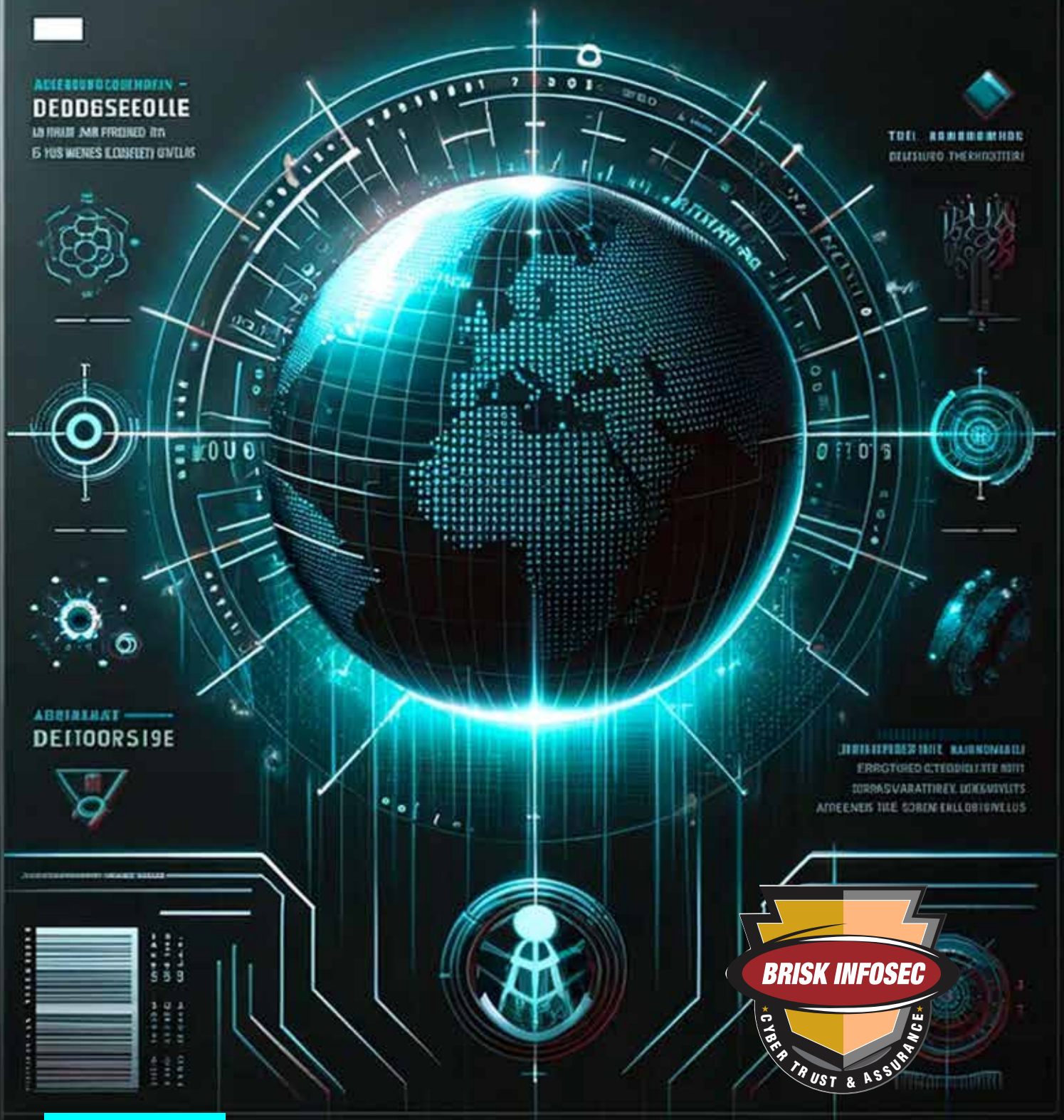
THREATSPLOIT

ADVERSARY REPORT



Edition-65

www.briskinfosec.com

Introduction :

In a landscape increasingly dominated by technology's pervasive influence, the specter of cyber threats grows ever more intricate and impactful. At Briskinfosec, we emphasize the critical importance of comprehending these threats. Our latest Cyber Insights report delves extensively into the digital realm, revealing trends, surfacing vulnerabilities, and offering profound insights into pivotal cyber events affecting diverse industries. This report aims to present a comprehensive perspective on current trends, forecast potential trajectories, and illuminate the wider repercussions for both enterprises and individuals navigating through this digital epoch.

The past few weeks have witnessed a surge in high-impact cyber incidents, amplifying concerns across various sectors and regions. The threat landscape has been punctuated by a series of sophisticated attacks, each posing unique risks and challenges to global cybersecurity.

Notably, a widespread JavaScript (JS) malware strain has indiscriminately affected over 50,000 users across the banking sector globally, raising alarms about the pervasiveness of financial cyber threats. Simultaneously, the infiltration of the notorious PikaBot malware through malvertising campaigns disguised within popular software installations has added complexity to the cybersecurity terrain.

Additionally, vulnerabilities within WordPress (WP) plugins have exposed e-commerce platforms to grave risks of credit card theft, signifying the dire consequences of unpatched software vulnerabilities. Meanwhile, the sentencing of members associated with the LAPSUS$ teen hacking group for their orchestrated attacks underscores the legal repercussions in combating cybercriminal activities.

Moreover, the RusticWeb malware's targeted assault on Indian government entities has triggered operational alerts, drawing attention to the geopolitical ramifications of cyber intrusions. Not to be overlooked, Microsoft's recent warning concerning the 'FalseFont' backdoor threat has heightened concerns regarding covert infiltration techniques and the need for vigilance against sophisticated attack vectors.

These recent cyber incidents serve as poignant reminders of the evolving threat landscape, urging organizations and individuals to fortify defenses, stay vigilant, and collaborate in the pursuit of resilient cybersecurity measures.

Best regards,
Briskinfosec Threat Intelligence Team.

Contents :

NKN Blockchain Targeted by NKAbuse DDoS Malware

A new threat, NKAbuse, uses blockchain in NKN to launch DDoS attacks, infiltrate systems via Apache Struts flaw, and operate as a backdoor on Linux, primarily targeting devices in Colombia, Mexico, and Vietnam. Its blockchain use makes detection and control challenging, posing a serious concern for security.

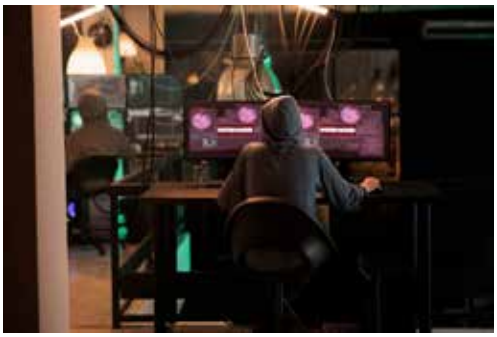
Attack Type : Peer-to-Peer Implant

Cause of Issue : Blockchain Exploitation

Domain Name : Cloud-Based Software

APT29 Targets JetBrains TeamCity Servers

Widespread attacks on unpatched JetBrains TeamCity servers by APT29, a Russian-linked group, exploit CVE-2023-42793 for remote code execution. The SVR leverages this to infiltrate networks, conduct espionage, and deploy backdoors like GraphicalProton, targeting diplomatic agencies globally. Additionally, Microsoft disclosed multiple Russian-linked cyber intrusions, including assaults on Ukraine's agriculture sector, employing malware like SharpWipe, alongside influence operations shaping the Ukraine conflict's online narrative.



Attack Type : Supply Chain Exploitation

Cause of Issue : Cyber Espionage

Domain Name : Software Companies

APAC Firms Under Siege : GambleForce's SQL Attacks

A new hacker group, GambleForce, conducts SQL attacks targeting Asia-Pacific sectors like gambling and government, exploiting system vulnerabilities. They breach organizations, accessing sensitive data via open-source tools, emphasizing the need for secure coding and updated software to prevent such breaches.

Attack Type : SQL Injection

Cause of Issue : Cyber espionage

Domain Name : Software Development Companies

KV-Botnet Strikes Cisco, DrayTek & Fortinet : Stealth Attacks

KV, a complex botnet discovered by Black Lotus Labs at Lumen Technologies, infiltrates major router brands, covertly transferring data since February 2022. Linked to China's Volt Typhoon, it targets high-profile entities, complicating detection via in-memory operation, affecting critical U.S. utilities, and eluding tracking through common devices.

Attack Type : Covert Infiltration

Cause of Issue : Cyber infiltration

Domain Name : Software Companies

WordPress 6.4.2 Patch : Critical Remote Attack Fix

WordPress released version 6.4.2 to fix a critical security flaw. Threat actors could exploit this by combining it with other bugs in plugins/themes to execute harmful code on vulnerable sites. Users are urged to update to the latest version immediately. Developers should consider using safer alternatives than the 'unserialize' function in their projects.

Attack Type : Code Injection

Cause of Issue : Security patch

Domain Name : Software Development Companies

ColdFusion Flaw Breaches Federal Servers

Unpatched Adobe ColdFusion vulnerability (CVE-2023-26360) exploited by unknown threat actors targeting government servers. Attacks led to compromised systems, malware deployment, and attempts at data theft, highlighting the urgency of software updates for security.

Attack Type : Remote Code Execution

Cause of Issue : Software Patch

Domain Name : Software Development Companies

15k GitHub Go Module Repos Vulnerable to Repojacking

"Thousands of Go programming language modules on GitHub are vulnerable to an attack called repojacking, allowing bad actors to create fake repositories due to username changes or deletions. This poses a risk of supply chain attacks. Additionally, exposed API tokens on platforms like GitHub and Hugging Face, including those from major companies, raise concerns about potential exploitation for various attacks."

Attack Type : Supply Chain

Cause of Issue : GitHub Risks

Domain Name : Software Development Companies

Kimsuky Strikes : S. Korean Research in Crosshairs

North Korean groups, Kimsuky and Lazarus' Andariel, are up to no good. Kimsuky's after research institutes with phishing for backdoors, while Andariel's phishing crypto projects and stealing defense data in South Korea. Both are using shady tactics, from sanctions to ransomware.

Attack Type : Targeted Phishing

Cause of Issue : Cyber espionage

Domain Name : Software Development Companies

SLAM Vulnerability : “Spectre Strikes Intel, AMD, Arm CPUs”

Researchers revealed "SLAM," a new side-channel attack on Intel, AMD, and Arm CPUs, leveraging features like LAM, UAI, and TBI to extract sensitive kernel memory via Spectre-based methods. AMD advises current defenses, Intel plans guidance for upcoming processors, and Linux is working on patches to disable LAM. VUSec previously introduced "Quarantine" to isolate security domains on separate CPU cores, thwarting covert channels.

Attack Type : CPU Isolation

Cause of Issue : CPU Exploit

Domain Name : Manufacturing and Industrial Control Systems (ICS)

Router Flaws Threaten Critical Sectors

Several critical vulnerabilities in Sierra Wireless AirLink routers, used across vital sectors like healthcare, energy, and transportation, expose 86,000 devices to hackers. Exploitable flaws enable password theft, complete control takeover, and unauthorized access to crucial networks. While patches exist, outdated software leaves lingering risks, potentially allowing cybercriminals to exploit these weaknesses for system disruption, network infiltration, and significant cyber threats.

Attack Type : Remote Takeover

Cause of Issue : Security overhaul

Domain Name : Energy and Utilities

Zero-Click Outlook RCE Exploits : New Insights

"Vulnerabilities in Microsoft Windows allowed hackers to exploit Outlook without user interaction. Attackers leveraged address manipulation and malicious audio files to gain control. While these flaws were patched, they were exploited to breach email servers. Recommendations include microsegmentation adoption and security setting adjustments for improved defense against such attacks."

Attack Type : Combo Exploit

Cause of Issue : Outlook Vulnerabilities

Domain Name : Software Development Companies

QakBot Strikes : New Tactics Hit Hospitality

"Vulnerabilities in Microsoft Windows allowed hackers to exploit Outlook without user interaction. Attackers leveraged address manipulation and malicious audio files to gain control. While these flaws were patched, they were exploited to breach email servers. Recommendations include microsegmentation adoption and security setting adjustments for improved defense against such attacks."

Attack Type : Phishing Malware

Cause of Issue : Deceptive Threats

Domain Name : Healthcare Industry

Healthcare Cyber Threats : Debunking Myths

Healthcare data, especially Electronic Health Records (EHRs), commands high prices on the dark web, fetching up to $1,000 per record due to their irreplaceable nature, driving cyberattacks costing over $10 million per breach. Ransomware targets exploit healthcare's digital reliance, stressing the need for proactive defenses and understanding attackers' tactics to safeguard vulnerable systems.

Attack Type : Ransomware Exploits

Cause of Issue : Healthcare Risks

Domain Name : Healthcare Industry

MongoDB Security Breach : Customer Data Exposed

MongoDB is probing a security breach, granting unauthorized entry to their systems and exposing client data, but data within MongoDB Atlas remains unaffected. They urge vigilance against phishing, promote stronger authentication, and suggest password changes. Login problems on Atlas and Support Portal were fixed, unrelated to the security breach. Ongoing investigations aim to deliver more insights soon.

Attack Type : Data Breach

Cause of Issue : Security Breach

Domain Name : Software Companies

Cloud Atlas Targets Russian Agro & Research : Spear Phishing Alert

Cloud Atlas, a long-running cyber espionage group, has targeted Russian organizations using sneaky emails that exploit old Microsoft Office flaws. They've been doing this for years, changing tactics to avoid detection. Recently, they're linked to a tool called Decoy Dog, allowing remote control of infected computers and secret data transmission to an online account. Despite exposure attempts, they work hard to hide and spy on organizations without getting caught.

Attack Type : Spear Phishing with Malware

Cause of Issue : Cyber Espionage

Domain Name : Cloud-Based Software

WP Plugin Breach : E-Commerce Credit Card Risk

"Tricky hackers made a fake WordPress plugin that steals credit card info from online stores. They hide it well, making it tough to remove and sneakily create secret access.

They trick people by pretending it's a helpful fix for websites, but it's actually a sneaky tool to steal credit card details. These hackers have also stolen lots of money from online shops and are using tricky ads on Google and Twitter for cryptocurrency scams. They've already taken nearly $59 million from thousands of people."

Attack Type : Malicious Plugin

Cause of Issue : WordPress Vulnerabilities

Domain Name : Finance and Banking

Iranian Hackers' Telecom Espionage in Africa with MuddyC2Go

MuddyWater, an Iranian cyber group linked to the country's Ministry of Intelligence, employs sophisticated methods like phishing and exploiting software vulnerabilities to target Middle Eastern entities. They've recently used a new tool, MuddyC2Go, for remote access. Meanwhile, a group named Gonjeshke Darande, associated with Israel's Military Intelligence, disrupted Iran's infrastructure. Both actions reflect escalating cyber tensions between the two nations.

Attack Type : Cyber Espionage

Cause of Issue : Geopolitical Cyberconflicts

Domain Name : Telecommunications Sector

Xaro : Latest DJvu Ransomware Variant

A new type of ransomware called Xaro is spreading through fake software downloads. It encrypts files, demands a ransom, and steals sensitive data. Attackers target vulnerable computers and communicate with servers to download different malware. To stay safe, avoid downloading from unreliable sources and organizations should whitelist trusted apps.

Attack Type : Ransomware Infection

Cause of Issue : File Encryption

Domain Name : Industrial Control Systems (ICS)

McDonald’s Ice Cream Machine Hackers' Startup Demise

Kytch, fixing McDonald's ice cream machines, faces closure due to alleged safety concerns by McDonald's. Emails imply machine manufacturer Taylor collaborated against Kytch. Amid legal battles, Kytch aims to reveal a conspiracy involving Taylor, Middleby, and McDonald's in a May trial.

Attack Type : Security Breach

Cause of Issue : Legal Disputes

Domain Name : Manufacturing Industry

Israeli Hackers Target 70% of Iran's Gas Stations

The hacking group, Gonjeshke Darande, claimed an Iran gas station cyberattack in response to perceived aggression. Affiliated with Iran's Revolutionary Guard, it targets Iranian entities, sparking investigations and media coverage, though Israel hasn't officially responded.

Attack Type : Cyber Espionage

Cause of Issue : Geopolitical Cyberstrike

Domain Name : Private Sector

Chameleon Trojan Evades Biometrics

Chameleon Android malware now targets UK and Italy, using Zombinder to spread. Masquerading as Google Chrome, it manipulates Android 13 settings, bypassing security via biometric tricks. Google Play Protect aims to counter these evolving threats, while Zimperium flags 29 malware families hitting 1,800 banking apps across 61 countries.

Attack Type : Android Banking Malware

Cause of Issue : Sophisticated Malware

Domain Name : Finance and Banking

Banking Growth Hinges on Cyber-Resilience : SBI Chief

The FE BankNXT conclave featured banking tech leaders discussing India's banking growth. SBI's Nitin Chugh emphasized cybersecurity and praised India's digital infrastructure. He envisioned a future AI-driven bank focusing on responsible data usage. The event, powered by ServiceNow, concluded in Mumbai.

Attack Type : Cyber Breach

Cause of Issue : Banking Conclave

Domain Name : Finance and Banking

ICMR's Data Leak Silence : Unanswered Questions

A major data breach at India's ICMR caused widespread concern, involving data from 81.5 crore individuals. Despite this, the institution has stayed silent. Questions arise about the breach's validity and ICMR's response plan. Concerns focus on prevention, detection, and accountability. Experts highlight the need for clarity on the breach's duration and origin. There's a call for transparency to uphold trust in digital health initiatives.

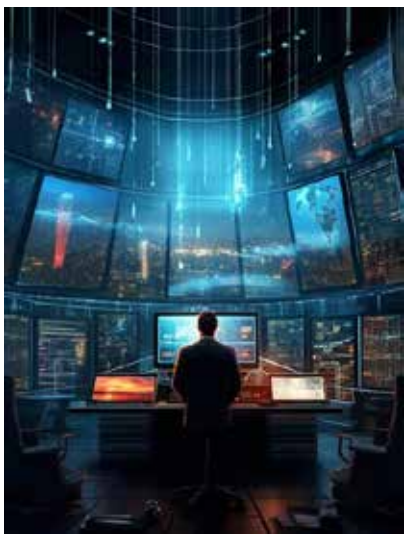
Attack Type : Data Breach

Cause of Issue : Transparency Urgent

Domain Name : Healthcare Industry

Data Security : Fueling Business Growth

Data security is crucial for Indian businesses facing soaring breach costs. Adherence to new laws, aligning leadership, and integrating security in tech and operations are vital. Proactive vulnerability assessments and leveraging tech like Generative AI are urged for faster threat detection, highlighting data's role beyond protection.



Attack Type : Data Security Emphasis

Cause of Issue : Data Protection

Domain Name : Software Development Companies

JS Malware Hits 50K+ Users Across Global Banks

Cybercriminals are actively using JavaScript malware to steal banking credentials from over 40 financial institutions worldwide. They're also running scams, like fake crypto services and phishing sites mimicking postal services, raking in millions. These threats underscore the need for caution online, especially regarding banking information and suspicious links.

Attack Type : JavaScript Credential Theft

Cause of Issue : Online Threats

Domain Name : Finance and Banking

PikaBot Malvertising : Popular Software Disguise

A malware called PikaBot is now spread through fake ads while people search for real software like AnyDesk. This sneaky program lets bad actors take over computers and install more harmful tools. They use tricks to avoid being caught, like redirecting from Google to a fake site and checking if the victim's computer is real. This kind of attack has been seen before, suggesting a shared method among cybercriminals. There's also a rise in attacks through web browsers, introducing new threats that steal sensitive information.

Attack Type : Malicious Adware

Cause of Issue : Misleading software

Domain Name : Software Development Companies

WP Plugin Exposes E-Commerce to Credit Card Theft

A deceptive WordPress plugin used in Magecart attacks on e-commerce sites aims to steal credit card details during checkout, posing removal challenges. This follows warnings on fake security patches creating unauthorized access. Another Magecart campaign and misleading ads fuel concerns about credit card theft and cryptocurrency scams, resulting in significant losses.

Attack Type : Magecart Skimming

Cause of Issue : Magecart Malware

Domain Name : Finance and Banking

LAPSUS$ Teen Members Sentenced for Attacks

British teens from LAPSUS$ cybercrime group faced consequences for high-profile attacks on firms. One received hospital order, other youth rehab, targeting companies with tactics like SIM swapping, Telegram extortion. LAPSUS$ linked to larger cyber entity, warning on risks of youthful tech exploration.

Attack Type : Cyber Extortion

Cause of Issue : Illegal Consequences

Domain Name : Media and Entertainment

RusticWeb Malware Hits Indian Gov : Operation Alert

A phishing campaign called Operation RusticWeb is targeting Indian government and defense sectors with Rust-based malware to steal sensitive documents. The attack, linked to known groups tied to Pakistan, uses phishing emails with malicious files to gather data. These tactics resemble previous attacks, and it follows the discovery of the DoNot Team using a malicious Android app to spy on individuals in Kashmir, underscoring ongoing threats in sensitive regions.

Attack Type : Phishing Malware

Cause of Issue : Cyber Espionage

Domain Name : Manufacturing and Industrial Control Systems (ICS)

Microsoft Warns of 'FalseFont' Backdoor Threat

APT33 targeted Defense Industrial Base (DIB) with FalseFont backdoor. Israel accused Iran and Hezbollah of hacking Ziv Hospital via phishing with CVE-2023-46747.

Attack Type : Backdoor Attack

Cause of Issue : Cyber Attacks

Domain Name : Software Development Companies

Briskinfosec Technology and Consulting Pvt ltd,
No : 21, 2nd Floor, Krishnama Road,
Nungambakkam, Chennai - 600034, India.

Office : +044 4352 4537 | Mobile : +91 86086 34123
contact@briskinfosec.com | www.briskinfosec.com