Threatsploit

Adversary Report

Edition-70

Proud to be Recognized..!

Magazines : CIO World India, TLG

BRISKINFOSEC
CYBER TRUST & ASSURANCE

ET CISO.in

decrypt

2024 and Beyond : New Paradigms in Cybersecurity

June 27th

Meet us @ Mumbai

Sofitel BKC | Booth No : S9

www.briskinfosec.com

Introduction :

Dear Readers,

Welcome to the June 2024 edition of the Threatsploit Adversary Report, your indispensable source for the latest developments and emerging threats in the cybersecurity landscape. As we navigate through an era of unprecedented digital transformations across a multitude of industries, the complexity and frequency of cyber threats continue to evolve, becoming increasingly sophisticated and significantly disruptive.

This edition provides an extensive overview of recent cybersecurity incidents that have impacted diverse sectors including technology giants, financial institutions, healthcare providers, and government agencies. Notable incidents highlighted include intricate cyber-espionage campaigns, the emergence of next-generation malware attacks, and highly sophisticated social engineering tactics that have led to significant breaches and substantial data losses.

Our report meticulously analyzes each case to reveal the specific nature of the threat, the intricate mechanisms of the attacks, and the types of vulnerabilities that were exploited. By dissecting these incidents, we aim to provide a clear picture of the current threat landscape and the evolving tactics of cyber adversaries.

We encourage our readers to delve into the detailed descriptions provided, which are designed to enhance your understanding of each threat and its implications. With the Threatsploit Adversary Report as your guide, remain informed and vigilant as you navigate through the complex and ever-changing cyber threat environment.

Best regards,

Briskinfosec Threat Intelligence Team.

Report Inside :

1. Top Cyberattacks in the Last 30 Days :
A sector-by-sector breakdown of the most critical threats.

2. Top 5 Bug Bounty Programs :
Discover the most rewarding programs that are helping to secure the digital world.

3. Top 5 Cybersecurity Communities :
Join the conversation and enhance your cybersecurity knowledge with these vibrant communities.

Cyber Criminals Exploit GitHub and FileZilla to Deliver Malware Cocktail

A campaign named GitCaught, likely by Russian-speaking CIS actors, abuses GitHub, FileZilla, Bitbucket, and Dropbox to distribute stealer malware and banking trojans like Vidar and Lumma. The attack uses fake profiles and repositories to host counterfeit software, targeting Android, macOS, and Windows. This broad, cross-platform strategy utilizes overlapping C2 infrastructure to increase efficiency. Microsoft warns of the ongoing macOS threat, Activator, distributed via disk image files to steal data and disable security features.

Attack Type : Supply Chain

Cause of Issue : Exploitation of Legitimacy

Industry Type : Software Development Companies

Grandoreiro Banking Trojan Resurfaces, Targeting Over 1,500 Banks Worldwide

Global resurgence of Grandoreiro banking trojan post-January takedown involves large-scale phishing via malware-as-a-service (MaaS), targeting 1,500+ banks across 60+ countries. Significant malware updates enhance evasion and functionality, including Outlook integration for spreading spam emails. Trojan's methods include large file sizes to evade detection and geographic restrictions to avoid certain regions and systems.

Attack Type : Phishing Malware

Cause of Issue : Malware Resurgence

Industry Type : Finance and Banking

China-Linked Hackers Adopt Two-Stage Infection Tactic to Deploy Deuterbear RAT

China-linked BlackTech group deploys Deuterbear RAT in cyber espionage across Asia-Pacific. RAT evolves from Waterbear with advanced capabilities like shellcode plugins and HTTPS C&C communication. Concurrently, UNK_SweetSpecter campaign targets U.S. AI organizations with SugarGh0st RAT via AI-themed phishing, aiming possibly at stealing GenAI-related data.

Attack Type : Cyber Espionage

Cause of Issue : Unauthorized Access

Industry Type : Government Sector

Cybercriminals Exploiting Microsoft's Quick Assist Feature in Ransomware Attacks

Storm-1811, a financially motivated cybercriminal group, exploits Microsoft's Quick Assist for social engineering attacks, posing as IT support to install malicious tools like QakBot and Cobalt Strike. This enables them to deploy Black Basta ransomware across targeted industries since mid-April 2024. Microsoft is enhancing Quick Assist with warnings to combat these scams, emphasizing the need for vigilance and employee training against such tactics.

Attack Type : Social Engineering

Cause of Issue : Exploited Feature

Industry Type : Software Development Companies

Northern California city suffers second cyberattack in less than a month

St. Helena, California, experienced a cyberattack prompting shutdowns of city systems and the public library. The attack compromised over 20 computers and a network server. Law enforcement, including the FBI and Secret Service, are investigating. City files were backed up before the attack, ensuring data safety despite disruptions.

Attack Type : Ransomware Attack

Cause of Issue : Malware Infiltration

Industry Type : Telecommunications

Australians prescription records breached in large-scale ransomware attack

MediSecure, an e-prescription processing company in Australia, suffered a ransomware attack, prompting government intervention. While personal and health data were impacted, the extent of the breach remains unclear. Authorities are investigating, with initial indications pointing to a breach through a third-party vendor. This incident underscores the critical need for robust cybersecurity measures in the healthcare sector to safeguard patient data and trust in digital health services.

Attack Type : Ransomware Attack

Cause of Issue : Third-Party Breach

Industry Type : Pharmaceuticals and Biotechnology

Hackers Exploiting WP-Automatic Plugin Bug to Create Admin Accounts on WordPress Sites

Threat actors are exploiting CVE-2024-27956, a critical SQL injection flaw in the ValvePress Automatic plugin for WordPress, enabling site takeovers. The vulnerability, impacting versions prior to 3.92.0, allows unauthorized database access and creation of admin accounts. Attackers aim to maintain access by creating backdoors and obfuscating code, with over 5.5 million attack attempts detected since disclosure. Additionally, severe vulnerabilities in other plugins like Email Subscribers and Forminator pose risks of data extraction and remote code execution.

Attack Type : SQL Injection

Cause of Issue : Database Exploitation

Industry Type : Software Development Companies

Australian government investigating 'large-scale ransomware

MediSecure, a provider of electronic prescribing services, is at the center of a large-scale ransomware breach, impacting personal and health information. The company has taken immediate steps to mitigate the incident, believing it originated from a third-party vendor. Authorities are coordinating a response, including the Australian Digital Health Agency and the national cyber security coordinator. The breach raises concerns about data security in electronic health systems, echoing past incidents like the 2022 Medibank hack.

Attack Type : Ransomware Attack

Cause of Issue : Cyber Intrusion

Industry Type : Government Sector

Black Basta Ransomware Strikes 500+ Entities Across North America, Europe, and Australia

The Black Basta ransomware group has targeted over 500 entities in critical sectors since April 2022, using double-extortion tactics involving data encryption and exfiltration. The group employs phishing, known vulnerabilities, and various tools like Cobalt Strike for lateral movement. Evidence suggests ties to FIN7, and their attacks have increasingly impacted healthcare organizations. Law enforcement efforts have led to an 18% decline in ransomware activity in Q1 2024, with LockBit likely to rebrand due to reputational issues.

Attack Type : Double-Extortion

Cause of Issue : Phishing Vulnerabilities

Industry Type : Software Development Companies

Ransomware Attacks Exploit VMware ESXi Vulnerabilities in Alarming Pattern

Ransomware attacks on VMware ESXi infrastructure follow a consistent pattern involving initial access through phishing or vulnerabilities, privilege escalation, ransomware deployment, and backup deletion or encryption. Organizations are advised to implement robust monitoring, authentication, and backup strategies to mitigate these threats. A recent campaign uses malicious ads to distribute trojanized installers for WinSCP and PuTTY, leading to ransomware deployment. The ransomware scene sees turbulence with new families emerging and a decline in LockBit's prominence.

Attack Type : Ransomware Attack

Cause of Issue : Misconfiguration

Industry Type : Software Development Companies

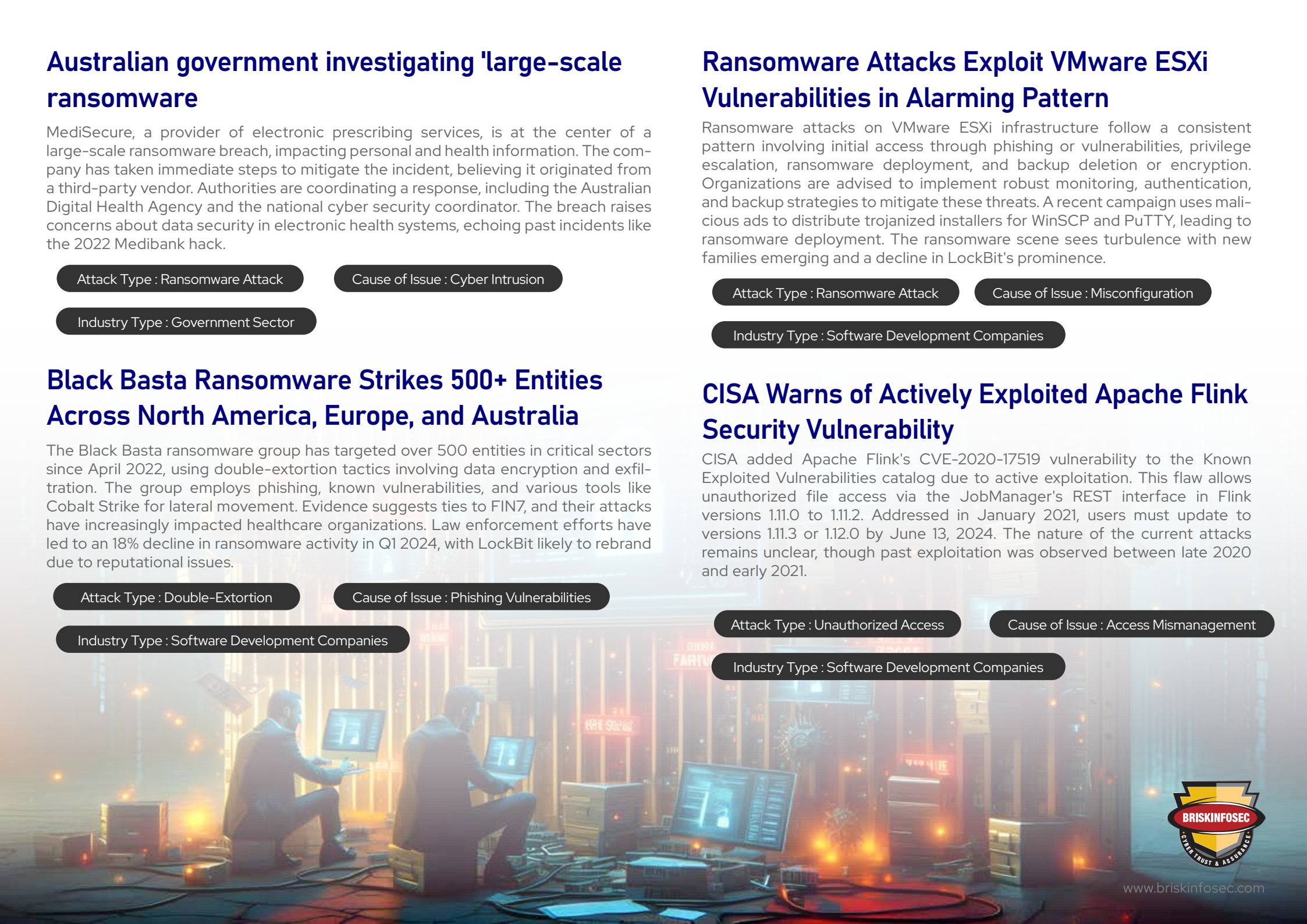
CISA Warns of Actively Exploited Apache Flink Security Vulnerability

CISA added Apache Flink's CVE-2020-17519 vulnerability to the Known Exploited Vulnerabilities catalog due to active exploitation. This flaw allows unauthorized file access via the JobManager's REST interface in Flink versions 1.11.0 to 1.11.2. Addressed in January 2021, users must update to versions 1.11.3 or 1.12.0 by June 13, 2024. The nature of the current attacks remains unclear, though past exploitation was observed between late 2020 and early 2021.

Attack Type : Unauthorized Access

Cause of Issue : Access Mismanagement

Industry Type : Software Development Companies



Ivanti Patches Critical Remote Code Execution Flaws in Endpoint Manager

Ivanti has patched multiple critical vulnerabilities in Endpoint Manager (EPM) and Avalanche, including SQL injection flaws allowing remote code execution. These affect versions prior to 2022 SU5. Additionally, high-severity issues were fixed in Neurons for ITSM, Connect Secure, and Secure Access clients. Meanwhile, a critical flaw in Netflix's Genie OSS could enable remote code execution via path traversal, impacting versions before 4.3.18. The U.S. government has warned of ongoing exploitation attempts targeting directory traversal vulnerabilities in software systems.

Attack Type : Remote Code Execution

Cause of Issue : SQL Injection

Industry Type : Software Development Companies

Google Patches Yet Another Actively Exploited Chrome Zero-Day Vulnerability

Google has patched a critical zero-day vulnerability, CVE-2024-4947, in Chrome related to a type confusion bug in the V8 engine. This marks the third zero-day fix within a week, highlighting its severity. Users should update to Chrome version 125.0.6422.60/.61 on Windows and macOS, or 125.0.6422.60 on Linux to secure against potential exploits. Chromium-based browser users are also urged to apply updates promptly.

Attack Type : Type Confusion

Cause of Issue : Misinterpreted Types

Domain Name : Software Industry

Iranian MOIS-Linked Hackers Behind Destructive Attacks on Albania and Israel

An Iranian threat group, attributed to the Ministry of Intelligence and Security (MOIS), known as Void Manticore or Storm-0842, has conducted destructive cyber attacks using wiper malware against targets in Albania and Israel. They collaborate with other groups like Scarred Manticore, using tactics such as exploiting vulnerabilities, deploying web shells, and conducting data exfiltration. The attacks combine psychological warfare with data destruction, aiming at governmental and organizational targets.

Attack Type : Destructive Malware

Cause of Issue : Sate-Sponsored Attacks

Industry Type : Manufacturing and Industrial Control Systems (ICS)

Kremlin-Backed APT28 Targets Polish Institutions in Large-Scale Malware Campaign

APT28, a Russia-linked nation-state actor, has conducted a large-scale malware campaign targeting Polish government institutions. The campaign involves convincing email content leading recipients to click on links redirecting to seemingly benign websites like Mocky and webhook.site, which serve as conduits for downloading malicious files disguised as image and script files. Once executed, these files facilitate data exfiltration and potentially enable remote control of compromised systems, reflecting APT28's sophisticated tactics in cyber espionage.

Attack Type : Malware Campaign

Cause of Issue : Sophisticated Phishing

Industry Type : Software Development Companies

Microsoft Outlook Flaw Exploited by Russia's APT28 to Hack Czech, German Entities

APT28, linked to Russia's GRU, conducted long-term cyber espionage campaigns targeting Czechia and Germany using vulnerabilities like CVE-2023-23397 in Microsoft Outlook. The attacks aimed at political entities, state institutions, and critical infrastructure, highlighting Russia's ongoing cyber threats denounced by NATO and the EU. Similar tactics include using botnets and DDoS attacks to influence elections and disrupt global democratic processes.

Attack Type : Cyber Espionage

Cause of Issue : Vulnerability Exploitation

Industry Type : Media and Entertainment

Critical GitHub Enterprise Server Flaw Allows Authentication Bypass

"GitHub patched a critical flaw (CVE-2024-4985) in GHES that could enable attackers to bypass authentication protections on instances using SAML single sign-on with encrypted assertions. This could lead to unauthorized access and provisioning of administrator privileges. The issue affects versions prior to 3.13.0, prompting GitHub's recommendation for affected organizations to update to patched versions (3.9.15, 3.10.12, 3.11.10, 3.12.4) to mitigate potential security risks."

Attack Type : Authentication bypass

Cause of Issue : SAML Misconfiguration

Industry Type : Software Industry

Cyberattack on Ascension leads to ambulance diversions

Ascension, a healthcare provider operating over 140 hospitals across the U.S., experienced a ransomware attack on May 8, 2024, impacting its network systems and electronic health records (EHR). Emergency medical services were diverted at some hospitals, and non-emergency procedures were paused as the organization switched to manual processes. Ascension is working with cybersecurity firms like Mandiant and governmental agencies to restore operations, emphasizing transparency and patient care amidst ongoing recovery efforts.

Attack Type : Ransomware Attack

Cause of Issue : Cybersecurity Breach

Industry Type : Healthcare Industry

GHOSTENGINE Exploits Vulnerable Drivers to Disable EDRs in Cryptojacking Attack

A new cryptojacking campaign named REF4578, also known as HIDDEN SHOVEL, utilizes vulnerable drivers to disable Endpoint Detection and Response (EDR) solutions. Dubbed Bring Your Own Vulnerable Driver (BYOVD), this tactic aims to evade detection and sustain a persistent presence for deploying the XMRig miner and other malicious activities. The sophisticated attack involves complex steps like exploiting PowerShell scripts disguised as image files to download payloads and disable security measures, highlighting evolving threats in cybersecurity.

Attack Type : Cryptojacking Campaign

Cause of Issue : Driver Vulnerabilities

Industry Type : Software Development Companies

Malware Delivery via Cloud Services Exploits Unicode Trick to Deceive Users

A new phishing campaign named CLOUD#REVERSER is utilizing Google Drive and Dropbox to distribute malicious payloads. Attackers send phishing emails containing ZIP archives with executables disguised as legitimate files like Excel documents using Unicode tricks to deceive users. Once executed, the malware downloads and runs obfuscated VBScript and PowerShell scripts from cloud services, enabling persistent access and command execution on compromised systems. This tactic highlights a growing trend of threat actors leveraging trusted platforms to evade detection and maintain long-term control over targeted networks.

Attack Type : Phishing Campaign

Cause of Issue : File Deception

Industry Type : (SaaS) Providers

Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack

CNA Financial, a major U.S. insurance firm, experienced a sophisticated cyber attack in March 2021, disrupting services for three days. The attack involved ransomware and impacted corporate email and network systems, prompting the company to shut down as a precautionary measure. While investigations are ongoing to determine the full scope, CNA restored operations with enhanced security measures and is monitoring for any data compromises that could affect policyholders. The incident highlights ongoing concerns about cyber insurance firms being targeted for potentially lucrative data access by cybercriminals.

Attack Type : Ransomware Attack

Cause of Issue : Data Breach

Industry Type : Insurance Sector

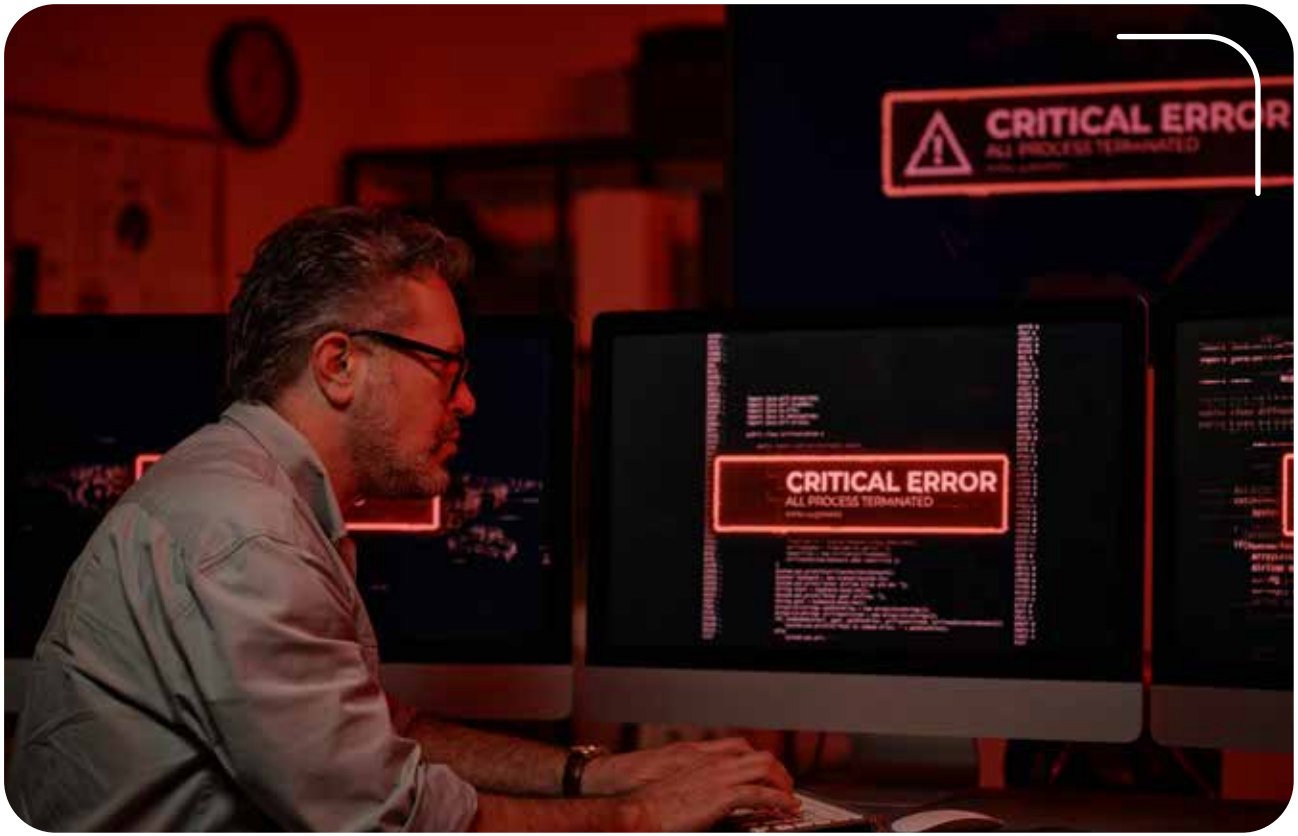
Tackling Cybersecurity Threats in the Biotechnology Industry

Biotechnology and life science organizations face increasing cybersecurity threats, driven by the value of their research and development data. Ransomware attacks surged during the pandemic, impacting sectors like pharmaceuticals with significant financial consequences. Benchling's R&D Cloud platform enhances collaboration and data management in biotech, emphasizing robust security measures to protect intellectual property. Moving forward, adopting cloud-based security strategies and leveraging economies of scale will be crucial to safeguarding sensitive data amidst advancing scientific discoveries.

Attack Type : Ransomware Attack

Cause of Issue : Cyber Threat

Industry Type : Pharmaceuticals and Biotechnology



Kerala's cooperative banks and hospitals prime target of hackers from Pakistan, China

In Kerala, cooperative banks, hospitals, and chit funds are under siege from cyber-attacks, primarily exploiting their IT vulnerabilities. Hackers, often from foreign countries like China and Pakistan, target these institutions due to inadequate security and outsourced IT management. Techniques like SQL injection are used to steal data, including patient records from hospitals. Even prestigious institutions like the Regional Cancer Centre have fallen victim, emphasizing the urgent need for enhanced cybersecurity measures across the board.

Attack Type : SQL Injection

Cause of Issue : Security Breach

Industry Type : Banks and hospitals

Ebury Botnet Malware Compromises 400,000 Linux Servers Over Past 14 Years

The Ebury botnet, active since 2009, has compromised over 400,000 Linux servers, with more than 100,000 still compromised as of late 2023. Managed by cybercriminals, Ebury targets servers for financial gain through activities like spam distribution, web traffic redirection, and stealing credentials. It includes sophisticated tools like HelimodSteal for credit card theft and HelimodRedirect for ad redirection, often exploiting SSH and web panel vulnerabilities. Despite efforts to disrupt it, Ebury remains a significant threat globally, demonstrating advanced capabilities in server-side malware operations.

Attack Type : Server-side Malware

Cause of Issue : Security Vulnerabilities

Industry Type : Software Developments Companies

CISA hit by hackers, key systems taken offline

The Cybersecurity and Infrastructure Security Agency (CISA) was hacked due to vulnerabilities in Ivanti products, compromising two systems. The compromised systems include the Infrastructure Protection (IP) Gateway and the Chemical Security Assessment Tool (CSAT). Although the attackers are not officially identified, reports suggest Chinese nation-state actors. CISA is taking steps to modernize and secure their systems in response to the breach.

Attack Type : Vulnerability Exploitation

Cause of Issue : Software Flaws

Industry Type : Government Sector

Fallout From Cyberattack at Ascension Hospitals Persists, Causing Delays in Patient Care

A cyberattack on Ascension, a major U.S. health system, forced doctors and nurses to revert to paper records, delaying patient care. The ransomware attack, attributed to the Black Basta group, compromised critical systems and highlighted vulnerabilities in healthcare cybersecurity. Ascension is working with federal agencies to address the breach and restore digital access, but the attack has disrupted operations and raised concerns about patient data security. Similar to a previous attack on Change Healthcare, this incident underscores the significant risks posed by cyberattacks on large healthcare organizations.

Attack Type : Ransomware Attack

Cause of Issue : Security Vulnerabilities

Industry Type : Healthcare Sector

Hackers Created Rogue VMs to Evade Detection in Recent MITRE Cyber Attack

The MITRE Corporation disclosed details of a recent cyber attack targeting its infrastructure in late 2023. Exploiting zero-day vulnerabilities in Ivanti Connect Secure (ICS), threat actors, identified as UNC5221, created rogue virtual machines within MITRE's VMware environment. This tactic aimed to evade detection by using compromised vCenter Server access to deploy backdoors and web shells, facilitating persistent access and data exfiltration. MITRE recommends enabling secure boot and utilizing specialized tools to detect and mitigate such stealthy threats effectively.

Attack Type : VMware Compromise

Cause of Issue : Zero-day Exploits

Industry Type : Software Development Companies

Experts Find Flaw in Replicate AI Service Exposing Customers' Models and Data

Researchers discovered a critical security flaw in Replicate, an AI-as-a-service provider, allowing potential access to AI models and sensitive data. Exploiting the vulnerability could lead to unauthorized access to customer AI prompts and results. The issue involved rogue containers and remote code execution, leveraging infrastructure weaknesses. Replicate has addressed the flaw, mitigating risks of data exposure from cross-tenant attacks on its platform.

Attack Type : Remote Code Execution

Cause of Issue : Security Flaw

Industry Type : Software Development Companies

MS Exchange Server Flaws Exploited to Deploy Keylogger in Targeted Attacks

Unknown actors are exploiting Microsoft Exchange Server vulnerabilities, including ProxyShell flaws, to deploy keylogger malware across government agencies, banks, IT firms, and educational institutions in Africa and the Middle East. The keylogger captures credentials and stores them in a file accessible via a specific internet path, impacting organizations in multiple countries since 2021. Organizations are advised to update Exchange Server, monitor for signs of compromise on the server's main page, and delete any compromised files storing stolen data to mitigate risks.

Attack Type : Keylogger Deployment

Cause of Issue : Keylogger Malware

Industry Type : Cloud-Based Software as a Service (SaaS) Providers

New Wi-Fi Vulnerability Enables Network Eavesdropping via Downgrade Attacks

Researchers discovered CVE-2023-52424, a Wi-Fi vulnerability dubbed SSID Confusion in IEEE 802.11 standards. It tricks users into connecting to a spoofed network, compromising their traffic. All Wi-Fi clients are affected, and mitigation involves updating authentication protocols and avoiding credential reuse across SSIDs.

Attack Type : SSID Spoofing

Cause of Issue : SSID Deception

Industry Type : Software Development Companies

Top 5 Bug Bounty Programs

1. HackerOne

HackerOne is a leading platform connecting organizations with a global community of security researchers to identify and resolve security vulnerabilities. It offers substantial rewards and supports a wide range of industries.

https://www.hackerone.com/

2. Bugcrowd

Bugcrowd is a prominent bug bounty platform that helps organizations manage vulnerability disclosure and bug bounty programs. It leverages a community of skilled researchers to find and fix vulnerabilities efficiently.

https://www.bugcrowd.com/

3. GitHub Security Lab

GitHub Security Lab aims to inspire and enable the global security research community to secure the world's code. It rewards security researchers for finding vulnerabilities in open source projects hosted on GitHub.

https://securitylab.github.com/

4. Microsoft Bug Bounty Programs

Microsoft's bug bounty programs cover a wide range of products, including Windows, Office, and Azure. The programs are known for offering high rewards, sometimes up to $250,000 for critical cloud vulnerabilities.

https://www.microsoft.com/en-us/msrc/bounty

5. Google Vulnerability Reward Program (VRP)

Google's VRP incentivizes security researchers to find and report vulnerabilities in Google's products, such as Android, Chrome, and Google Cloud. The program is notable for its generous payouts and broad scope.

https://bit.ly/Google_Vulnerability_Reward_Program

Top 5 Cybersecurity Communities

1. Black Hat

Widely recognized for its global conferences, Black Hat is pivotal in the cybersecurity domain, presenting cutting-edge research, security trends, and vulnerabilities that shape the industry.

https://www.blackhat.com/

2. DEF CON

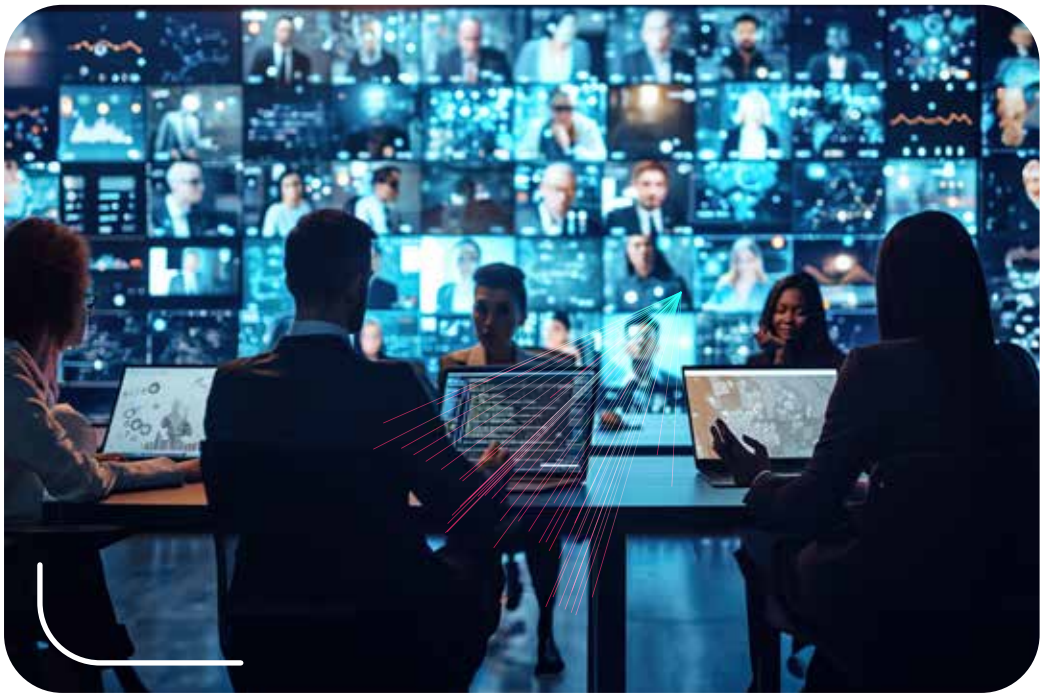
One of the oldest and largest hacker conventions in the world, DEF CON is a cornerstone of the hacking community, offering a platform for security professionals and hobbyists to collaborate and share knowledge.

https://defcon.org/

3. SANS Institute

Known for its extensive training programs and courses, SANS Institute is a leading provider of cybersecurity education and certification to professionals across the globe.

https://www.sans.org/



4. OWASP (Open Web Application Security Project)

OWASP plays a crucial role in improving software security across industries. It provides comprehensive resources and tools freely available, making it a fundamental resource for web application security.

https://owasp.org/

5. MITRE:

Through its management of federally funded research and development centers and initiatives like the CVE (Common Vulnerabilities and Exposures) system, MITRE has a significant impact on national and international cybersecurity standards and practices.

https://www.mitre.org/

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**