TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 21, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In today's dynamic digital landscape, defending against cyber threats has emerged as a critical priority for organisations worldwide. With these threats evolving constantly, companies are not just focused on safeguarding their data but also on reinforcing the fundamental frameworks that drive modern business operations. The goal is to establish resilience against an ever-expanding array of emerging threats.

Elevate your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory. Gain invaluable insights into the most recent cyber risks and implement proactive strategies to strengthen your defences, effectively mitigating potential vulnerabilities.

INTRODUCTION | MINECRAFT SOURCE PACK SPREADS MALWARE | CERT-IN ISSUES ADVISORY | MALWARE SPREAD THROUGH GOOGLE ADS | CYBERCRIMINALS EXPLOIT ROUTERS | MALICIOUS CODE DISGUISED AS CRACK | VULNERABILITIES IN BIG-IP CENTRAL MANAGER | GOOGLE SEARCH ADS DISTRIBUTE MALWARE | RANSOMWARE LAUNCHES GLOBAL ATTACK | RANSOMWARE USES DOUBLE EXTORTION TACTICS | DOJ INDICTS SEVEN HACKERS

Crafted Minecraft source pack distributes zEus stealer malware

A recent advisory cautions gamers about the security risks associated with game customisation, focusing on the zEus stealer malware in the Minecraft source pack. Hiding itself in innocuous downloads like Windows screensavers, the malware spreads through a WinRAR self-extract file, avoiding detection. Once activated, it stealthily collects personal information, including IP numbers, browser logins, Discord tokens, and more, organising the stolen information before sending it to a remote server.

This highlights the dangers of downloading from seemingly harmless sources and emphasises the need for strong security measures within the gaming community. To counter such threats, users should download only from reliable sources, use multi-factor authentication (MFA), and stay vigilant against suspicious activity.

ATTACK TYPE	Malware	SECTOR	Gaming industry
REGION	Global	APPLICATION	Windows

Source- https://www.fortinet.com/blog/threat-research/zeus-stealer-distributed-via-crafted-minecraft-source-pack

CERT-In issues advisory on critical security vulnerabilities

CERT-In issued an advisory highlighting critical security vulnerabilities in Microsoft Edge (Chromium-based), Progress Flowmon, and the WP Automatic WordPress plugin. Microsoft Edge vulnerabilities, rated high, could lead to unauthorised access and arbitrary code execution. Progress Flowmon's critical vulnerability, rated severe, enables remote, unauthenticated access and arbitrary command execution via API requests. The WP Automatic WordPress plugin's flaw, also rated severe, allows attackers to create administrator accounts and inject malicious SQL queries.

As these vulnerabilities expose systems to potential exploits, users must take preventive measures to safeguard their systems and data. Prompt software updates are recommended to mitigate these risks and strengthen cybersecurity defences.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Microsoft Edge, WordPress

Source- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2024-0154

Source- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2024-0153

INTRODUCTION | MINECRAFT SOURCE PACK SPREADS MALWARE | CERT-IN ISSUES ADVISORY | MALWARE SPREAD THROUGH GOOGLE ADS | CYBERCRIMINALS EXPLOIT ROUTERS | MALICIOUS CODE DISGUISED AS CRACK | VULNERABILITIES IN BIG-IP CENTRAL MANAGER | GOOGLE SEARCH ADS DISTRIBUTE MALWARE | RANSOMWARE LAUNCHES GLOBAL ATTACK | RANSOMWARE USES DOUBLE EXTORTION TACTICS | DOJ INDICTS SEVEN HACKERS

D3F@ck Loader malware spreads through Sponsored Google Ads

Cybersecurity experts have uncovered a novel threat called D3F@ck Loader, which has spread through sponsored Google ads since March 2024. Priced at $70 per day and $490 a week, it bypasses major security protocols and distributes malware like Raccoon Stealer and Danabot. It leverages Extended Validation (EV) certificates to enhance trustworthiness and evade detection by security programs like Microsoft's SmartScreen.

The attack vector involves malicious websites disguised as legitimate applications, emphasising caution when clicking on ads, even on reputed platforms. The loader's ability to bypass prominent security features highlights the importance of robust security measures and user education. Recommendations include implementing endpoint detection and response (EDR) solutions, conducting phishing and security awareness training (PSAT), and exercising least privilege to mitigate potential damage from malware infections.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://www.esentire.com/blog/d3f-ck-loader-the-new-maas-loader

Cybercriminals exploit routers to build proxy botnets

Cybercriminals and nation-state actors are targeting unsuspecting home and office routers to build anonymising proxy botnets. These botnets enable attackers to hide their identities while carrying out phishing scams, cryptocurrency mining, and other online threats. A recent FBI operation dismantled a large botnet built on compromised Ubiquiti EdgeRouters, highlighting the seriousness of the issue. Alarmingly, some of these devices have been compromised since 2016, demonstrating the long-term persistence of these threats.

Cybercriminals often lease compromised routers to fellow criminals and offer them to commercial residential proxy providers. Nation-state actors like Sandworm deploy their dedicated proxy botnets, whereas APT group Pawn Storm uses a criminal proxy botnet composed of Ubiquiti EdgeRouters. Security experts urge network defenders and home users to be vigilant, as weak default security settings and frequently overlooked software updates make routers easy targets. Recommendations include keeping router firmware up to date, limiting unnecessary internet exposure, and being mindful of signs of compromise on routers.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source- https://www.trendmicro.com/en_us/research/24/d/router-roulette.html

Attackers distribute malicious code disguised as crack

Cybercriminals are tricking users into installing malicious software disguised as cracks for popular applications like Hangul, Windows, and Microsoft Office. These threats target users downloading software cracks, causing large-scale infections on domestic networks in Korea. These fake cracks can steal user data, mine cryptocurrency for the attacker's benefit, and turn computers into proxy servers. The attackers keep their infection rate high by registering the task scheduler on infected systems so that they can execute PowerShell commands to install malware. They often release new malware variants to avoid detection.

Although the V3 product cleans task schedulers, systems remain vulnerable with new malware continually being installed. Users must exercise caution when downloading executable files from data-sharing sites and obtain software from official sources only. Updating security products like the V3 is crucial for blocking malware infections. For already infected systems, installing the V3 product can help clean task schedulers and prevent further malware installation.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://asec.ahnlab.com/ko/65307/

BIG-IP Central Manager vulnerability grants admin control to attackers

F5 has addressed high-severity vulnerabilities in their BIG-IP Next Central Manager, posing risks of administrative control and unauthorised account creation on managed assets. The vulnerabilities, including SQL and OData injection flaws within the API, allow remote execution of malicious commands if left unpatched. These vulnerabilities impact F5's latest flagship product line, representing a significant threat to network security. Attackers can exploit these flaws to gain administrative control and create hidden accounts on managed devices, posing persistent threats.

While no active exploits have been reported, F5 recommends access restriction and offers temporary mitigations. F5 has released fixes in software version 20.2.0 and advises immediate upgrades. Given the critical nature of these vulnerabilities, users are urged to exercise caution and implement additional security measures. Network security teams should enforce strict access controls and consider layered defences to enhance infrastructure protection.

ATTACK TYPE	Vulnerability	SECTOR	Global
REGION	Global	APPLICATION	F5 BIG-IP

Source- https://eclypsium.com/blog/big-vulnerabilities-in-next-gen-big-ip/

INTRODUCTION | MINECRAFT SOURCE PACK SPREADS MALWARE | CERT-IN ISSUES ADVISORY | MALWARE SPREAD THROUGH GOOGLE ADS | CYBERCRIMINALS EXPLOIT ROUTERS | MALICIOUS CODE DISGUISED AS CRACK | VULNERABILITIES IN BIG-IP CENTRAL MANAGER | GOOGLE SEARCH ADS DISTRIBUTE MALWARE | RANSOMWARE LAUNCHES GLOBAL ATTACK | RANSOMWARE USES DOUBLE EXTORTION TACTICS | DOJ INDICTS SEVEN HACKERS

Hackers leverage Google search ads to spread MSI-packed malware

Recent investigations have revealed a sophisticated cyberattack exploiting Google search ads to spread malware via Microsoft Installer (MSI) packages. This campaign employs a malware loader called FakeBat, which camouflages itself as legitimate software downloads to target unsuspecting users. The operation uses fraudulent ads, phishing sites, and advanced PowerShell scripts to deploy the malicious zgRAT malware, effectively compromising affected devices. The PowerShell scripts can also establish communication with malicious infrastructures and deliver subsequent payloads.

While researchers have successfully traced and blocked this operation, they emphasise the importance of implementing robust security measures and continuous monitoring to counter such threats. Users are advised to exercise caution online and to employ preventive measures such as limiting the use of MSIX files and maintaining updated security protocols.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://www.threatdown.com/blog/fakebat-05-05-2024/

Black Basta ransomware targets over 500 global organisations

The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI have disclosed that the Black Basta group, functioning as a Ransomware-as-a-Service (RaaS) operation, breached over 500 organisations worldwide between April 2022 and May 2024. The targets include high-profile victims like government contractors and healthcare institutions. A collaborative report from the Department of Health and Human Services (HHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) highlights the group's strategic targeting and sophisticated tactics, impacting critical infrastructure.

The advisory emphasises the urgent need for robust cybersecurity measures, particularly within vulnerable sectors like healthcare. Defenders are urged to adopt preventive measures outlined in the joint advisory to mitigate the risk of Black Basta ransomware attacks.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	North America, Australia, Europe	**APPLICATION**	Windows

Source- https://www.bleepingcomputer.com/news/security/cisa-black-basta-ransomware-breached-over-500-orgs-worldwide/

Trinity ransomware emerges with double extortion tactics

A new ransomware strain named Trinity employs a double extortion method, encrypting files and threatening data leaks. Trinity's resemblance with Ransomware "2023Lock" in ransom note structure and core codebase hints at a possible derivative or evolved form of 2023Lock. Additionally, parallels between Trinity and Venus ransomware, including registry value patterns and mutex naming conventions, imply a potential link or shared origin between the two strains. Venus ransomware, active since 2022, has been involved in numerous global cyberattacks.

The Trinity ransomware operators leverage both victim support and data leak websites. Its emergence shows a trend towards more sophisticated and coordinated ransomware attacks. Cybersecurity experts recommend preventive measures to mitigate such threats, including cautious handling of email attachments, regular offline backups, and maintaining updated software and security tools. In the event of an attack, immediate steps such as disconnecting infected devices and inspecting system logs are advised.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://cyble.com/blog/in-the-shadow-of-venus-trinity-ransomwares-covert-ties/

DOJ indicts seven linked to hacking group APT31

The U.S. Department of Justice has indicted seven individuals linked to APT31, a Chinese state-sponsored hacking group, for computer intrusions and wire fraud. APT31, also known as ZIRCONIUM, is associated with China's Ministry of State Security and engages in cyber espionage, targeting critics of China, U.S. businesses, and political figures. The group's tactics include spear-phishing campaigns, malware deployment, and exploiting vulnerabilities.

APT31's recent activities involved over 10,000 malicious emails targeting U.S. government officials, political figures, and businesses. Notably, APT31 has ties to the Hubei State Security Department and employs sophisticated malware like Cobalt Strike. Security experts recommend educating staff, updating software, implementing multi-factor authentication, monitoring for suspicious activity, and collaborating to mitigate APT31's threats effectively.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source- https://socradar.io/dark-web-profile-apt31/

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today’s cyber threat landscape.

Book your visit

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.