TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 11, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Today's digital environment demands robust cybersecurity. As threats evolve constantly, organisations must prioritise data protection, build resilience, and secure their core operational frameworks swiftly. Staying vigilant of cyberattack trends and prompt implementation of security measures is crucial for every organisation to mitigate cyber risks.

Leverage Tata Communications' weekly threat intelligence advisory to gain invaluable insights into the most recent cyber threats. This report empowers you to implement proactive cybersecurity strategies and effectively mitigate potential vulnerabilities.

Bondnet botnet uses miner bots as C2 servers

The Bondnet botnet continues its operations with novel techniques. First exposed by GuardiCore in 2017, the botnet was detailed further by the DFIR Report in 2022 for targeting SQL Server with XMRig miners. Recent analysis reveals that Bondnet attackers have created reverse RDP environments for high-performance bots since 2023. These environments use a modified FRP tool and a Cloudflare tunnelling client to establish Command and Control (C2) servers.

Experts noted that after failing to convert victim systems to C2, the attackers continued their operation with different bots and possibly alternative programs. This persistent evolution highlights Bondnet's resilience and ongoing threat, requiring continuous vigilance and updated defence mechanisms from cybersecurity professionals.

ATTACK TYPE	Malware	**SECTOR**	IT, Hcare/Hosp, Finserv, MFG, Construction, Govt, Oil and gas, BFSI, AUTO/MFG, TELCO
REGION	Global	**APPLICATION**	Generic

Source- https://asec.ahnlab.com/ko/65885/

Moonstone Sleet linked to ransomware attacks

Microsoft has attributed recent FakePenny ransomware attacks to the North Korean hacking group Moonstone Sleet. Known for demanding millions in ransom, Moonstone Sleet has developed distinct methods despite initial similarities with other North Korean groups. Previously tracked as Storm-17, the group targets financial and cyberespionage sectors, employing advanced tactics such as trojan software, malicious games, and fake companies to engage with potential victims. They have evolved from using shared malware techniques to creating their own bespoke infrastructure.

In April, Moonstone Sleet deployed FakePenny ransomware, demanding $6.6 million in Bitcoin. This financial motivation and their ongoing espionage efforts indicate the dual threat they pose. Microsoft's analysis highlights Moonstone Sleet's adaptation and expansion of tactics, marking a significant development in North Korean cyberoperations.

ATTACK TYPE	Cyberespionage	SECTOR	Manufacturing, Government
REGION	Global	APPLICATION	Generic

Source- https://www.bleepingcomputer.com/news/microsoft/microsoft-links-moonstone-sleet-north-korean-hackers-to-new-fakepenny-ransomware/

Critical vulnerability identified in Fortinet's SIEM solution

Security researchers have exposed a severe command injection vulnerability, CVE-2024-23108, in Fortinet's SIEM solution, patched in February. This vulnerability affects FortiSIEM versions 6.4.0 and higher. Despite initial confusion over its classification, Fortinet acknowledged it as a variant of a previously fixed flaw. The flaw allows unauthenticated execution of remote commands as the root user.

Horizon3 recently released a proof-of-concept exploit for this flaw. Horizon3's technical analysis revealed the exploit's method and potential impact, highlighting the critical nature of the vulnerability. Fortinet vulnerabilities, often exploited in cyberattacks, highlight the importance of timely patching of applications to secure corporate and government networks from threats like ransomware and espionage.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Fortinet

Source- https://www.bleepingcomputer.com/news/security/exploit-released-for-maximum-severity-fortinet-rce-bug-patch-now/

SharpPanda APT group targets entities with sophisticated malware

Security experts have uncovered a sophisticated malware campaign by the SharpPanda APT group, targeting Malaysian entities in early 2024. Disguised as a Microsoft Word document, the malware established a backdoor for unauthorised access. It used XOR decryption to evade detection, collected extensive system information, and communicated with a Command and Control (C2) server in Hong Kong using encrypted data.

The malware, detected on VirusTotal in April, posed as a legitimate file to deceive users, achieving a high detection score on antivirus software. The campaign highlights the persistent threat of state-sponsored actors and the urgent need for heightened vigilance and robust security measures to protect against such sophisticated attacks.

ATTACK TYPE	Malware	**SECTOR**	IT, Hcare/Hosp, Finserv, MFG, Construction, Govt, Oil and gas, Aerospace, Def. Ind., E-Com, BFSI, Chem. Mfg., TELCO
REGION	Malaysia	**APPLICATION**	Windows

Source- https://notes.netbytesec.com/2024/05/inside-sharppandas-malware-targeting.html

Citrix Workspace flaw grants root access

Analysts have issued an urgent advisory for a high-severity vulnerability in the Citrix Workspace app for Mac, identified as CVE-2024-5027. This flaw enables local attackers to escalate privileges to the root level, risking data theft, system modification, or complete system takeover. The vulnerability affects versions before 2402.10.

Citrix has proactively provided patches and detailed update instructions to customers and partners to address this issue. Users are strongly urged to update to version 2402.10 or later to mitigate the risk. The update, released on 23 May 2024, supports macOS 11 Big Sur through macOS 14 Sonoma. Users are also encouraged to subscribe to security alerts for future updates.

ATTACK TYPE	Vulnerability	SECTOR	IT, Hcare/Hosp, Finserv, MFG, Constr., Govt, Oil and gas, Aerospace, E-Com, BFSI, TELCO
REGION	Global	APPLICATION	Citrix Workspace

Source- https://cybersecuritynews.com/citrix-workspace-app-vulnerability/

Sophisticated malware packer targets Linux systems

Cybersecurity researchers have uncovered the exploitation of the Kiteshield packer by various cyber threat actors, targeting Linux environments. Groups like Winnti and DarkMosquito use Kiteshield to achieve low detection rates of ELF files on VirusTotal. Kiteshield employs advanced evasion techniques, including multi-layered encryption and anti-debugging strategies, challenging detection and analysis. The packer's RC4 encryption, XOR obfuscation, and anti-debugging tactics significantly hinder static and dynamic analysis. The versatility of Kiteshield presents a significant challenge for cybersecurity defenders, highlighting the evolving threat landscape in Linux environments.

Initially linked to less sophisticated attackers, Kiteshield is now favoured by high-profile threat groups. Analysts have revealed that Kiteshield-packed files contain a loader section that decrypts the payload, using complex mechanisms to maintain stealth. The increasing use of Kiteshield emphasises the urgent need for improved detection and analysis methods to defend against these sophisticated attacks.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Linux

Source- https://securityonline.info/kiteshield-packer-emerges-as-a-significant-threat-in-linux-malware-landscape/

Kimsuky group exploits MS Office vulnerability for keylogger attacks

Cybersecurity experts have identified the Kimsuky attack group distributing keylogger malware by exploiting a long-known vulnerability in the MS Office formula editor (CVE-2017-11882). This flaw allows the attackers to deploy the malware by executing a malicious script through mshta. The malicious script, masked as an error page, initiates the malware installation. This includes creating and hiding files and attempting to register for re-execution via registry keys. Despite a coding error preventing full execution, the script still gathers and transmits sensitive information. The malware collects and transmits system and user data to a command-and-control server.

Experts stress the importance of applying security patches, updating software regularly, and using advanced security solutions to mitigate such threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source- https://asec.ahnlab.com/ko/66135/

Fake browser updates spread BitRAT and Lumma Stealer malware

In May 2024, researchers uncovered a sophisticated malware campaign distributing BitRAT and Lumma Stealer through fake browser updates, which were delivered via compromised web pages. Users visiting these pages triggered the automatic download of malicious ZIP archives containing PowerShell scripts and .NET loaders. These scripts employed advanced techniques, including AMSI bypasses and encryption to deploy and maintain the malware. This highlights the escalating threat from such fake update schemes.

The BitRAT malware provides extensive remote access capabilities, while Lumma Stealer targets sensitive data, including cryptocurrency wallets and 2FA extensions. Experts urge users to maintain vigilance, apply security patches, and employ robust security solutions to prevent such sophisticated attacks. Experts also recommend using up-to-date antivirus software and conducting phishing and security awareness training to mitigate these risks.

ATTACK TYPE	Malware	**SECTOR**	IT, Hcare/Hosp, Finserv, MFG, Construction, Govt, Oil and gas, Business, E-Com, BFSI, Airlines and Aviation, Chem. Mfg., TELCO
REGION	Global	**APPLICATION**	Generic

Source- https://www.esentire.com/blog/fake-browser-updates-delivering-bitrat-and-lumma-stealer

TATA COMMUNICATIONS

AllaSenha malware strikes the banking sector

A recent cyberattack has targeted Brazilian banks with the "AllaSenha" malware, designed to steal banking credentials. Security experts revealed that the malware, a variant of the AllaKore RAT, uses Azure cloud services for command and control. The campaign targets banks, including Banco do Brasil, Bradesco, and Itaú Unibanco, using phishing emails to distribute a malicious Windows shortcut file disguised as a PDF. Upon execution, this file downloads further malicious payloads via PowerShell scripts.

AllaSenha, developed in Python with a Delphi-based loader, employs sophisticated techniques to steal credentials and two-factor authentication codes. Operational mistakes of the attackers have exposed their identities, linking them to previous criminal activities. The campaign highlights the persistent threat to Latin American financial institutions. Cybersecurity experts urge users to apply security patches and remain vigilant against phishing attacks.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	Brazil	**APPLICATION**	Windows

Source- https://thehackernews.com/2024/05/brazilian-banks-targeted-by-new.html

Cyberespionage group LilacSquid targets global business sectors

Emerging cyberespionage group LilacSquid has been linked to data theft attacks across various sectors in the U.S., Europe, and Asia since 2021. Their sophisticated operations involve exploiting vulnerabilities and using compromised RDP credentials to infiltrate targets. LilacSquid's campaign aims to establish long-term access to victim organisations and steal valuable data through attacker-controlled servers. The group targets IT firms in the U.S., energy companies in Europe, and the pharmaceutical sector in Asia.

Their methods include deploying custom malware like PurpleInk and leveraging the open-source MeshAgent tool. PurpleInk is highly obfuscated and versatile, capable of running applications, performing file operations, and launching remote shells. Recent variants are streamlined for reverse shell creation and data transfer. Overlaps with North Korean APT groups, such as Andariel and Lazarus, suggest LilacSquid's sophistication and potential connections to established espionage entities.

ATTACK TYPE	Malware	**SECTOR**	Pharmaceuticals, IT, Energy
REGION	Europe, Asia, United States	**APPLICATION**	Windows

Source- https://thehackernews.com/2024/05/cyber-espionage-alert-lilacsquid.html

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