TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: June 4, 2024

TATA COMMUNICATIONS

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.

Turla group leverages MSBuild to deliver backdoor

Analysts have identified a sophisticated cyberattack campaign that uses compromised LNK files distributed through spam emails to target individuals with lures such as invitations to human rights seminars. Upon execution, these LNK files initiate a PowerShell script that uses MSBuild to deploy a fileless backdoor, enabling attackers to control infected systems. The final payload is similar to the TinyTurla backdoor, suggesting possible links to the Russia-based Turla APT group, notorious for targeting NGOs and using compromised web servers for command and control.

The campaign employs MSBuild project files and PDFs within the LNK files for hassle-free execution. The backdoor grants attackers remote control capabilities via a Command and Control (C&C) server. The presence of Russian-language comments and similar tactics further implicate the Turla group. This incident highlights the need for robust cybersecurity measures, including strong email filtering, caution with email attachments, restricted use of MSBuild, and network-level monitoring to detect unusual activities.

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

Source- https://cyble.com/blog/tiny-backdoor-goes-undetected-suspected-turla-leveraging-msbuild-to-evade-detection/

TATA COMMUNICATIONS

ShrinkLocker turns BitLocker into ransomware

A new ransomware strain, ShrinkLocker, is leveraging Windows BitLocker to encrypt data by creating new boot partitions. Written in VBScript, ShrinkLocker targets specific Windows versions, modifies system partitions, and secures infected systems by altering registry settings. Unlike typical ransomware, it does not leave a ransom note but uses contact emails as boot partition labels. The strain's destructive nature and deployment against government and corporate entities highlight the need for robust security measures.

Attackers exploit BitLocker, originally intended for data protection, to encrypt files. ShrinkLocker's sophisticated use of VBScript, Windows Management Instrumentation, and system utilities highlights the advanced skills of its developers. The attackers clear logs and encrypt entire drives, complicating forensic analysis. Effective mitigation includes strong encryption tool configuration, minimal user privileges, network traffic logging, and regular backups. This incident emphasises the importance of proactive security measures and behavioural analysis for detection.

ATTACK TYPE	Malware	**SECTOR**	Manufacturing, Government
REGION	Indonesia, Jordan, Mexico	**APPLICATION**	Windows

Source- https://securelist.com/ransomware-abuses-bitlocker/112643/

TATA COMMUNICATIONS

Novel threat Synapse distributed as Ransomware as a Service (RaaS)

In February 2024, Synapse ransomware emerged as a significant cyber threat, distributed as a Ransomware-as-a-Service (RaaS) on the dark web. SynapseCrypter, the ransomware payload, features rapid encryption, NTFS search, and selective encryption modes, sparing Iranian systems through time zone and language checks. Its advanced techniques include privilege escalation via access token theft and the use of custom algorithms to encrypt telemetry data sent to its command-and-control server.

Initial observations on a Russian hacker forum highlighted its capabilities, including flexible encryption modes and silent operation. SynapseCrypter's resemblance to the Babuk ransomware, following a 2021 source code leak, suggests possible code sharing or affiliation. Pre-encryption steps involve disabling security systems and deleting shadow copies, while post-encryption actions include file renaming and system modifications. This highlights the urgent need for organisations to enhance cybersecurity measures, employ robust endpoint protection, educate users, and develop comprehensive incident response plans to combat sophisticated ransomware attacks effectively.

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

Source- https://www.cyfirma.com/research/synapse-ransomware-technical-analysis/

Discord malware variant Iluria Stealer emerges

Cybersecurity experts are raising alarms over a new malware variant Iluria Stealer developed by Ykg, the developer behind Nikki Stealer and SonicGlyde. Managed by a team of four, Iluria Stealer version 2 uses an obfuscated Electron app to decrypt malicious code during runtime and steal Discord tokens and browser credentials. It then downloads a malicious JavaScript file to intercept account changes and send data to a command-and-control server. This enables hackers to ransom users or exploit their accounts for further attacks, including targeting crypto exchanges and bank accounts.

This highlights the urgent need for robust cybersecurity measures, regular updates, comprehensive employee training, strategic incident response plans, regular security audits, and collaboration with industry peers. Other recommendations include updating and patching systems, deploying cutting-edge endpoint protection, and implementing application whitelisting.

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

Source- https://www.cyfirma.com/research/iluria-stealer-a-variant-of-another-discord-stealer/

TATA COMMUNICATIONS

Rust-based ransomware Embargo leverages double extortion tactics

Analysts have identified a new ransomware variant Embargo, developed in Rust, which employs double extortion tactics, exfiltrating and encrypting sensitive data, and threatening to release it publicly if the ransom is unpaid. Embargo uses encryption algorithms like ChaCha20 and Curve25519 and operates via command-line arguments, disabling recovery, terminating specific processes, and excluding certain directories to ensure system operability. Embargo's leak site and log generation structure share similarities with ALPHV, which was dismantled by law enforcement in March 2024.

Embargo has so far disclosed details of four victims globally. The ransomware group initially demanded $1 million, threatening to notify victims' clients, employees, partners, and authorities upon non-payment. Embargo's development in Rust signifies a trend towards sophisticated cross-platform ransomware, necessitating cybersecurity measures such as regular backups, software updates, and the use of reputed internet security and antivirus software on connected devices such as mobiles, laptops, and PCs.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	VMWare ESXi, Windows, Linux

Source- https://cyble.com/blog/the-rust-revolution-new-embargo-ransomware-steps-in/

Operation Diplomatic Specter targets government entities

Chinese APT group TGR-STA-0043 is conducting an extensive cyber espionage campaign, Operation Diplomatic Specter, targeting governmental entities in the Middle East, Africa, and Asia. Active since late 2022, this campaign employs rare email exfiltration techniques and newly discovered backdoors, TunnelSpecter and SweetSpecter, to gather sensitive data on military operations, diplomatic missions, and foreign ministries. The group uses robust cryptographic algorithms and exploits known exchange server vulnerabilities for initial access. The APT group's activities reflect a strategic effort aligned with Chinese state interests, aiming to influence and monitor geopolitical developments worldwide.

Despite law enforcement efforts, such as the takedown of the ALPHV ransomware site in March 2024, the group remains persistent and adaptable, frequently regaining access and updating its tactics. This campaign emphasises the necessity for stringent cybersecurity measures, including regular updates and robust patch management, to protect sensitive information and mitigate espionage risks.

ATTACK TYPE	Malware, Cyberespionage	**SECTOR**	Government, Military
REGION	Middle East, Africa, Asia	**APPLICATION**	Windows

Source- https://unit42.paloaltonetworks.com/operation-diplomatic-specter

ESXi ransomware attacks unpatched VMware systems

Ransomware attacks on VMware ESXi infrastructure are rising, exploiting vulnerabilities and misconfigurations to gain access, escalate privileges, and deploy ransomware. These attacks often disrupt backups and exfiltrate data. Cybercriminals use tools like TMChecker and trojan installers, spread via malicious ads, complicating detection. Key threat actors include LockBit, HelloKitty, and BlackMatter. The attacks follow a typical pattern: gaining initial access through phishing or exploiting vulnerabilities, escalating privileges, deploying ransomware, compromising backups, and executing data exfiltration.

Researchers stress the importance of robust security measures, including comprehensive monitoring, stringent authentication, regular security patches, and maintaining secure and tested backups to ensure the resilience of digital infrastructures. Ensuring the collection and delivery of logs to Security Information and Events Management (SIEM) solutions can help in early detection. Also, strict network policies limiting access to essential entities can hinder lateral movement. By adopting these best practices, organisations can strengthen their defences against ransomware, safeguarding the integrity of systems.

ATTACK TYPE	Vulnerability, Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	VMWare ESXi

Source- https://www.sygnia.co/blog/esxi-ransomware-attacks/

Sharp Dragon targets government organisations

Since November 2023, Chinese cyber threat actor Sharp Dragon, previously known as Sharp Panda, has extended its cyber espionage campaign to Africa and the Caribbean, leveraging compromised networks in Southeast Asia. Using advanced tools like Cobalt Strike Beacon and compromised email accounts, Sharp Dragon aims to strengthen China's presence and influence in these regions, aligning with broader geopolitical objectives. Phishing attacks employing tailored lures have facilitated footholds in these new territories.

Sharp Dragon exploits 1-day vulnerabilities to compromise Command and Control (C2) operations infrastructure. The adjustments in Sharp Dragon's tactics, including carefully selecting targets, using publicly and readily available tools, adopting a Cobalt Strike Beacon over custom backdoors, and using EXE-based loaders, indicate a refined strategy for targeting high-profile government organisations. This strategic shift highlights China's concerted efforts to expand its cyber influence in regions that the global threat intelligence community has overlooked.

ATTACK TYPE	Malware	**SECTOR**	Govt
REGION	Africa	**APPLICATION**	Generic

Source- https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/

Cybercriminals use SmallTiger malware in domestic attacks

Recent cyberattacks associated with the SmallTiger malware have targeted South Korean firms in defence, automobile parts, and semiconductor manufacturing. Initially identified in November 2023, the attacks, linked to the Kimsuky group, involve lateral movement within networks. The attacks also deploy DurianBeacon, a backdoor malware previously confirmed in Andariel attacks, later evolving to SmallTiger.

The attackers resumed in February 2024, using new techniques for internal propagation. Methods include exploiting software update programs and using tools like Mimikatz and ProcDump to steal credentials. Recent incidents in May 2024 saw SmallTiger distributed via GitHub instead of traditional command and control servers. Companies are urged to enhance monitoring, apply security patches promptly, and be alert of suspicious email attachments and downloads to mitigate these sophisticated threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South Korea	**APPLICATION**	Generic

Source- https://asec.ahnlab.com/ko/65918/

Criminals use cloud storage for APT attacks

Recently, experts have reported cyberattacks that leverage cloud services like Google Drive, OneDrive, and Dropbox to distribute malware and collect user information. These attacks involve uploading remote access trojans (RATs) often disguised as legitimate files to cloud servers.

Experts have detailed how these attacks are carried out. Initially, LNK files disguised as HTML documents lure users to click on them. Once executed, these files decode Base64-encoded commands, save them as PowerShell scripts, and run them. These scripts download decoy documents such as fake police reports and other script files from the attackers' cloud storage, enabling information theft and system control. The attackers use Dropbox to host these files, using token-based authentication for access. Users are advised to verify file extensions and formats before execution to prevent infection.

ATTACK TYPE	Malware	**SECTOR**	IT, Healthcare/hospitals, Financial Services, MFG, Construction, Govt, Oil and gas, E-Comm, Airline, BFSI, AUTO/MFG, Telecommunications
REGION	Global	**APPLICATION**	Generic

Source- https://asec.ahnlab.com/ko/65684/

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