TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 15, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In a dynamic digital environment, individuals, businesses, and government entities are continuously facing complex cybersecurity challenges. These risks have the potential to disrupt regular operations, resulting in significant financial and reputational consequences. Therefore, it is crucial to bolster your digital defences and guard against cyber threats that could compromise the integrity, confidentiality, and availability of enterprise data.

Enhance your security measures by utilising our weekly reports, providing the latest cyber threat intelligence. Protect your IT assets from persistent threats through our comprehensive advisory services. In an era where cyber resilience is paramount, our cyber threat intelligence report equips your organisation with the essential knowledge to strengthen its security posture.

LemonDuck mines cryptocurrency

A recent report revealed a resurgence of the LemonDuck malware, now exploiting the EternalBlue vulnerability (CVE-2017-0144) in Microsoft's SMB protocol for cryptomining attacks. First exploited by WannaCry ransomware, EternalBlue remains a key entry point for malware like LemonDuck, which mines cryptocurrency by hijacking network resources while evading detection.

LemonDuck employs phishing, brute-force attacks, and SMB exploits to gain access to systems. Once compromised, it uses PowerShell to avoid detection, deploy payloads, and hijack processing power for cryptomining. Researchers noted that an attacker from Taichung City, Taiwan, exploited SMB services to gain administrative access, creating a hidden share for remote control. The malware uses a batch file (p.bat) to execute malicious actions, such as downloading additional malware and disabling Windows Defender. It then adds exclusions for the entire C: drive and the PowerShell process to ensure continued undetected operation.

ATTACK TYPE	Malware	**SECTOR**	IT, healthcare, financial services, manufacturing, construction, government, oil and gas, energy, defence, BFSI, mining, telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://securityonline.info/lemonduck-exploits-eternalblue-vulnerability-for-cryptomining-attacks/

DrayTek fixes router vulnerabilities

DrayTek has released security updates for multiple router models to address 14 vulnerabilities, including a critical remote code execution (RCE) flaw with a maximum CVSS score of 10. Discovered by Forescout Research's Vedere Labs, these vulnerabilities affect both supported and end-of-life models. Due to the high risk, DrayTek has provided patches for routers in both categories.

Forescout's scans revealed that around 785,000 DrayTek routers may be vulnerable, with over 704,500 exposing their web interfaces to the internet – interfaces that should be restricted to local access. The report also highlighted that nearly half of these vulnerable devices are in the US, with significant numbers in the UK, Vietnam, the Netherlands, and Australia, according to Shodan results. Users are urged to update their devices immediately to prevent potential exploitation.

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

Source - https://www.bleepingcomputer.com/news/security/draytek-fixed-critical-flaws-in-over-700-000-exposed-routers/

RCE flaws impact network switches

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning about two critical vulnerabilities in Optigo Networks ONS-S8 Aggregation Switches, widely used in critical infrastructure. These flaws could allow authentication bypass and RCE, posing a significant risk due to their low attack complexity and remote exploitability.

The first vulnerability, tracked as CVE-2024-41925, involves improper validation of user-supplied file paths, leading to PHP Remote File Inclusion (RFI). This allows attackers to perform directory traversal, bypass authentication, and execute arbitrary code. The second issue, CVE-2024-45367, results from weak password verification enforcement, enabling unauthorised access to the switch's management interface and sensitive data. Both vulnerabilities are rated as critical, with a CVSS score of 9.3. No fixes are currently available, so users are urged to implement the vendor's recommended mitigations. CISA advises organisations to monitor for suspicious activity and report incidents for tracking and analysis.

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

Source - https://www.bleepingcomputer.com/news/security/cisa-network-switch-rce-flaw-impacts-critical-infrastructure/

APT deploys backdoor and RAT

North Korean threat actors, likely linked to APT37 (also known as Reaper, InkySquid, and ScarCruft), have been found deploying a newly discovered backdoor and remote access trojan (RAT) called VeilShell. The campaign, dubbed SHROUDED#SLEEP, primarily targets Cambodia and other Southeast Asian nations. APT37, active since 2012 and affiliated with North Korea's Ministry of State Security (MSS), is known for cyberespionage activities, using malware like RokRAT (Goldbackdoor) and custom tools for covert intelligence gathering.

VeilShell is delivered via a ZIP file containing a malicious Windows shortcut (LNK), which launches PowerShell to install additional malware, including a lure document and malicious DLL files. Once installed, the backdoor grants attackers full control over compromised systems, enabling data exfiltration, registry modification, and task creation. This discovery follows a recent report that revealed a financially motivated campaign by another North Korean group, Andariel, targeting American organisations in August 2024.

ATTACK TYPE	Malware	**SECTOR**	IT, healthcare, financial services, manufacturing, construction, education, e-commerce, BFSI, automobile, software development
REGION	Southeast Asia	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/10/north-korean-hackers-using-new.html

Nitrogen malware targets organisations with innovative means

In November 2023, a BlackCat ransomware attack was traced back to Nitrogen malware hosted on a website impersonating the Advanced IP Scanner. A malicious ZIP file, downloaded from a fraudulent website, initiated the attack by executing Nitrogen, which deployed Sliver and Cobalt Strike beacons via Python scripts. Once inside the network, the attacker used tools like PowerSploit, SharpHound, and Impacket for lateral movement, harvesting domain credentials to expand control. They employed Restic, an open-source backup tool, to exfiltrate data from a file server to a remote server in Bulgaria.

Eight days after gaining initial access, the attacker modified a privileged user password and distributed the BlackCat ransomware across the network using PsExec and batch scripts. The ransomware was set to execute after rebooting systems into Safe Mode, leading to widespread file encryption. The entire intrusion spanned over eight days, with the ransomware deployment occurring approximately 156 hours after initial access. Six new rules were added to the Private Ruleset to address this attack.

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

Source - https://thedfirreport.com/2024/09/30/nitrogen-campaign-drops-sliver-and-ends-with-blackcat-ransomware/

Linux servers compromised by malware

A stealthy malware campaign targeting misconfigured and vulnerable Linux servers has been identified, delivering a malware dubbed “perfctl” to run cryptocurrency mining and proxyjacking software. Researchers have noted perfctl’s elusive nature, highlighting its ability to lie dormant when the server is in use and resume activity only when idle. Perfctl exploits a known vulnerability in Polkit (CVE-2021-4043) to escalate privileges, allowing it to deploy a cryptocurrency miner called “perfcc.” The malware also uses advanced techniques to evade detection, including deleting its binary after execution and mimicking legitimate system processes to blend in.

The malware spreads by exploiting vulnerable Apache RocketMQ instances and installs a rootkit for defence evasion. To minimise risk, it’s advised to regularly update systems, restrict file execution, enforce network segmentation, disable unused services, and apply role-based access control (RBAC) to protect critical files.

ATTACK TYPE	Malware	**SECTOR**	IT, healthcare, financial services, manufacturing, construction, government, oil and gas, energy, defence, BFSI, aviation, mining, telecommunications
REGION	Global	**APPLICATION**	Linux

Source - https://thehackernews.com/2024/10/new-perfctl-malware-targets-linux.html

Threat actors attack Asian entities with intricate malware

Researchers have uncovered several cybercampaigns targeting government institutions in Thailand since 2023, attributed to a new China-aligned APT group named CeranaKeeper. This group leverages updated versions of tools previously linked to Mustang Panda, as well as newly developed tools that exploit services like Pastebin, Dropbox, and GitHub to execute commands and steal sensitive documents.

CeranaKeeper has been active since early 2022, primarily targeting Asian countries, including Thailand, Myanmar, the Philippines, Japan, and Taiwan. Their tactics include turning compromised machines into update servers and using GitHub's pull request features to create stealthy reverse shells. They also employ single-use components to harvest entire file trees. Research indicates CeranaKeeper and Mustang Panda are distinct entities, although they may share some tools and information. The group's primary goal is data exfiltration, evolving its methods to remain undetected and maximise the extraction of sensitive files from compromised networks.

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

Source - https://www.welivesecurity.com/en/eset-research/separating-bee-panda-ceranakeeper-making-beeline-thailand/

Spear-fishing campaign creates headaches for organisations

A recent spear-phishing attack targeted recruitment offices, tricking them into downloading a fake resume that led to a more_eggs backdoor infection. This malware, part of the Golden Chickens malware-as-a-service (MaaS) toolkit, is known for its use by financially motivated threat groups like FIN6 and the Cobalt Group, typically targeting financial and retail institutions. More_eggs operates as a JScript backdoor, downloading additional payloads such as infostealers and ransomware.

The attack leveraged advanced social engineering tactics, including a convincing website and a malicious file disguised as a resume. Upon infection, the malware used Living Off the Land Binaries (LOLBins) like ie4uinit.exe to evade detection. Analysts isolated the compromised endpoint, blocked the attack's indicators of compromise (IOCs), and contained the infection before further damages occurred. Custom detection models and automated response capabilities proved critical in mitigating this evolving cyber threat.

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

Source - https://www.trendmicro.com/en_us/research/24/i/mdr-in-action--preventing-the-moreeggs-backdoor-from-hatching--.html

Botnet targets entities in over 100 countries

In September 2024, researchers detected an alarming surge in activity from a new botnet family called Gorilla Botnet. Between September 4 and 27, Gorilla Botnet issued over 300,000 attack commands, targeting more than 100 countries, with China and the US being the most impacted. Its targets spanned various sectors, including universities, government websites, telecoms, banks, gaming, and gambling.

Gorilla Botnet, a modified version of the Mirai botnet, supports multiple CPU architectures like ARM, MIPS, and x86. It incorporates advanced DDoS techniques and uses encryption methods like those employed by the KekSec group to conceal critical information. It also implements multiple persistence techniques, including modifying system files like /etc/inittab and /etc/profile, and ensuring the execution of malicious scripts during system startup or user login, demonstrating its high level of evasion and control over compromised IoT devices and cloud hosts.

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

Source - https://nsfocusglobal.com/over-300000-gorillabot-the-new-king-of-ddos-attacks/

Malicious scripts compromising Magneto, Adobe Commerce

Recent attacks exploiting CosmicSting vulnerabilities have escalated, now chaining with CNEXT to achieve RCE. Previously, attackers were injecting malicious scripts into CMS blocks, but this new tactic is more dangerous. CosmicSting (CVE-2024-34102) allows arbitrary file reading, and when combined with CNEXT (CVE-2024-2961), attackers can escalate privileges and take full control of unpatched systems.

Merchants using Adobe Commerce/Magento are urged to patch both vulnerabilities immediately. Adobe's troubleshooting guide offers mitigation steps, and a standalone tool is available to detect CNEXT. This attack involves establishing a WebSocket connection to wss://sellerstat.site/wss, allowing attackers to execute JavaScript remotely. Payloads delivered vary across affected stores but focus on stealing customer payment data through various injection techniques. The use of real-time communication enables attackers to dynamically adjust their payloads, making detection and mitigation considerably more difficult.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Magneto, Adobe Commerce

Source - https://sansec.io/research/cosmicsting-cnext-persistent-backdoor

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