TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 2, 2024

TATA

THREAT INTELLIGENCE ADVISORY REPORT

The digital world is constantly evolving, as are the cyber threats. Businesses around the world are prioritising data security and fortifying their core security systems. Organisations must stay informed about the latest cyberattack trends and promptly implement security updates. This will enable them to protect their assets from potential attacks.

Tata Communications’ weekly threat intelligence advisory is designed to give you that edge. Our report provides insights into the latest cyber risks, empowering you to take proactive steps to bolster your defences and efficiently address potential vulnerabilities.

Windows IIS server attacked by coin-mining malware

A recent cyberattack on a South Korean medical institution’s Windows IIS server has highlighted the vulnerabilities of unpatched web servers. Chinese-speaking attackers exploited the compromised server to install coin-mining malware.

In the initial attack, the attackers used web shells such as Chopper and Behinder and privilege escalation tools such as BadPotato. They used Cpolar for remote access and installed the XMRig coin miner. Days later, in the second attack, they used Certutil to download additional malware. The attackers also installed GodPotato, PrintNotifyPotato, and CVE-2021-1732 vulnerability malware to escalate privileges. Both attacks aimed to mine cryptocurrency, using various Chinese-developed tools and techniques. These incidents emphasise the urgent need for robust security measures, regular system updates, and vigilant monitoring to protect against such breaches.

ATTACK TYPE	Malware	SECTOR	Healthcare
REGION	South Korea	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/66860/

Malvertising campaign distributes Oyster backdoor

Researchers have uncovered a malvertising campaign distributing the Oyster backdoor malware through fake software installers. The campaign targets and leads unsuspecting users searching for popular downloads, such as Google Chrome and Microsoft Teams, to malicious websites mimicking legitimate platforms. In three incidents, users downloaded malware from typo-squatted sites resembling Microsoft Teams, which installed a malicious binary.

Oyster, also known as Broomstick, was first identified in September 2023. It collects information, communicates with command-and-control (C2) servers, and allows remote code execution. Analysts noted the direct deployment of Oyster Main without the typical loader. This campaign highlights the growing threat of malvertising. Users are urged to implement robust cybersecurity measures and to be cautious when downloading software.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://securityonline.info/malvertising-campaign-uses-fake-installers-to-spread-oyster-backdoor/

Phishing platform ONNX Store targets Microsoft 365 users

Analysts have identified ONNX Store, a phishing-as-a-service (PhaaS) platform, targeting Microsoft 365 accounts within the financial sector. The platform uses QR codes in PDF attachments to bypass two-factor authentication (2FA) and steal credentials. ONNX Store is managed using Telegram bots and offers various subscription tiers. Its phishing pages mimic real Microsoft 365 login interfaces, tricking victims into entering their authentication details.

Analysts believe the ONNX Store is a rebranded version of the Caffeine phishing kit, with significant overlaps in infrastructure and tactics. ONNX Store uses Cloudflare to prevent phishing domain shutdowns, exploiting legitimate anti-bot CAPTCHA features and IP proxying. Experts recommend blocking unverified attachments, employing FIDO2 security keys, and educating employees on the risks of embedded QR codes in PDF documents.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Global	APPLICATION	Windows

Source - https://blog.eclecticiq.com/onnx-store-targeting-financial-institution

Sophisticated Void Arachne campaign targets VPN users

A new threat dubbed Void Arachne is targeting Chinese-speaking users through malicious Windows Installer (MSI) files disguised as VPN software. The campaign, discovered in April 2024, uses SEO poisoning and social media platforms to distribute Winos 4.0 C2 framework and compromised MSI files embedded with deepfake pornography tools.

The campaign exploits the high demand for VPN services in China. The attackers lure users with advertisements for popular software such as LetsVPN, QuickVPN, and a Telegram language pack for simplified Chinese. They leverage black hat SEO tactics and Telegram channels to propagate backdoored installers. Winos 4.0 can perform keylogging, DDoS attacks, remote shell access, and more. The campaign highlights the growing threat to users in China seeking to bypass the Great Firewall.

ATTACK TYPE	Malware	SECTOR	Information technology, Healthcare, Manufacturing, Government, Oil and gas, Energy, Aerospace, Defence, Aviation, BFSI, Automotive, Mining, Telecommunications
REGION	China	APPLICATION	Windows

Source - https://thehackernews.com/2024/06/void-arachne-uses-deepfakes-and-ai-to.html

Hijack Loader campaign targets users with fake software

Cybercriminals target users with trojan software to deliver Hijack Loader malware. Researchers reported that attackers trick users into downloading password-protected archives containing fake Cisco Webex Meetings apps. These archives, once extracted and executed, launch Hijack Loader, which then drops Vidar Stealer via an AutoIt script.

This campaign uses DLL side-loading techniques to remain undetected and bypass User Account Control (UAC) for privilege escalation, allowing additional payloads like cryptocurrency miners to be installed. The malware adds itself to Windows Defender’s exclusion list for defence evasion. These attacks highlight the increasing sophistication of cyber threats and the need for vigilant cybersecurity measures.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://thehackernews.com/2024/06/cybercriminals-exploit-free-software.html

INTRODUCTION | COIN-MINER ATTACKS WEB SERVER | MALVERTISING CAMPAIGN SPREADS BACKDOOR | ONNX STORE TARGETS MICROSOFT 365 | VOID ARACHNE TARGETS VPN USERS | HIJACK LOADER ATTACKS USERS | MARKOPOLO TARGETS CRYPTO USERS | CYBERCRIMINALS EXPLOIT QR CODES | ATTACKERS EXPLOIT ZERO-DAY FLAWS | NEW DIAMORPHINE LINUX VARIANT EMERGES | ESPIONAGE CAMPAIGN TARGETS TELCOS

Malware by Markopolo targets cryptocurrency users

A cybercriminal known as Markopolo has launched a large-scale scam targeting cryptocurrency users through information-stealing malware. This sophisticated operation employs a fake virtual meeting software named Vortax, among other applications, to deploy malware such as Rhadamanthys and Atomic macOS Stealer (AMOS). Once installed, the malware steals sensitive information, including cryptocurrency wallet credentials.

Analysts noted that Markopolo employs agile strategies, quickly abandoning detected scams and pivoting to new tactics. This adaptability has enabled the cybercriminal to maintain the scam's effectiveness. The campaign has impacted users across multiple platforms, highlighting a significant rise in macOS security threats. The ongoing threat posed by information-stealing malware emphasises the need for robust cybersecurity measures, particularly for cryptocurrency users.

ATTACK TYPE	Malware	SECTOR	Information technology, Healthcare, Manufacturing, Construction, Government, Military, Oil and gas, Energy, Defence, Airline, BFSI, Mining, Telecommunications
REGION	Global	APPLICATION	macOS, Windows

Source - https://thehackernews.com/2024/06/warning-markopolos-scam-targeting.html

Cybercriminals exploit QR codes in sophisticated phishing campaign

QR code phishing campaigns are increasing in China. In a recently reported attack, threat actors impersonating the Ministry of Human Resources and Social Security targeted citizens with fake documents embedded with QR codes. Scanning the QR code directs the users to a phishing site that obtains their bank card details and passwords. The attackers use a Domain Generation Algorithm (DGA) to develop phishing URLs, creating difficulties in detection and blocking.

The campaign highlights the evolving tactics of cybercriminals, who leverage the popularity of QR codes in China to deceive unsuspecting victims. Users are advised to scan QR codes only from trusted sources, check URLs carefully, and use reputable antivirus and anti-phishing software. Educating the public about the risks associated with QR codes and maintaining updated security measures are crucial in protecting against these sophisticated phishing attacks.

ATTACK TYPE	Malware	SECTOR	All
REGION	China	APPLICATION	Windows

Source - https://cyble.com/blog/rising-wave-of-qr-code-phishing-attacks-chinese-citizens-targeted-using-fake-official-documents/

INTRODUCTION | COIN-MINER ATTACKS WEB SERVER | MALVERTISING CAMPAIGN SPREADS BACKDOOR | ONNX STORE TARGETS MICROSOFT 365 | VOID ARACHNE TARGETS VPN USERS | HIJACK LOADER ATTACKS USERS | MARKOPOLO TARGETS CRYPTO USERS | CYBERCRIMINALS EXPLOIT QR CODES | ATTACKERS EXPLOIT ZERO-DAY FLAWS | NEW DIAMORPHINE LINUX VARIANT EMERGES | ESPIONAGE CAMPAIGN TARGETS TELCOS

Cyberespionage group exploits zero-day vulnerabilities

The Chinese cyberespionage group UNC3886 has been misusing zero-day vulnerabilities in Ivanti, Fortinet, Ivanti, and VMware devices and maintains persistent access to compromised environments. This evasive group employs rootkits, backdoors, and credential-harvesting SSH clients to evade detection. These tools enable extended spying and data theft.

UNC3886 exploits zero-day flaws like CVE-2022-41328 (Fortinet FortiOS) and CVE-2022-22948 (VMware vCenter) to deploy malware, obtain credentials, and perform lateral movements within networks. The group's tactics include using rootkits like Reptile and Medusa on virtual machines. They also deploy backdoors such as MOPSLED and RIFLESPINE that exploit trusted services like GitHub and Google Drive for C2 operations. Organisations are advised to follow security recommendations from Fortinet and VMware to protect against these sophisticated threats.

ATTACK TYPE	Malware	SECTOR	Government, Energy, Aerospace, Defence
REGION	North America, Europe, Africa, Asia	APPLICATION	vCenter, Tools, FortiOS

Source - https://thehackernews.com/2024/06/chinese-cyber-espionage-group-exploits.html

INTRODUCTION | COIN-MINER ATTACKS WEB SERVER | MALVERTISING CAMPAIGN SPREADS BACKDOOR | ONNX STORE TARGETS MICROSOFT 365 | VOID ARACHNE TARGETS VPN USERS | HIJACK LOADER ATTACKS USERS | MARKOPOLO TARGETS CRYPTO USERS | CYBERCRIMINALS EXPLOIT QR CODES | ATTACKERS EXPLOIT ZERO-DAY FLAWS | NEW DIAMORPHINE LINUX VARIANT EMERGES | ESPIONAGE CAMPAIGN TARGETS TELCOS

New variant of Diamorphine Linux rootkit identified

A new variant of the Diamorphine Linux kernel rootkit with advanced functionalities has been discovered. This sophisticated version, identified in March 2024, mimics the legitimate x_tables Netfilter module, making it harder to detect. It includes features like device functionality to unload the rootkit and magic packets for arbitrary command execution.

Diamorphine, a well-known rootkit, hides files and folders, allowing attackers to maintain undetected access. The reported new variant targets Linux Kernel 5.19.17 and uses Netfilter hooks to avoid suspicion. Experts recommend keeping systems updated, using secure internet connections, avoiding untrusted downloads, and using robust cybersecurity solutions to prevent such infections.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source - https://decoded.avast.io/davidalvarez/new-diamorphine-rootkit-variant-seen-undetected-in-the-wild/

Malicious espionage campaign targets Asian telcos

A sophisticated cyberespionage campaign linked to Chinese state-sponsored groups has breached multiple telecom operators in an unnamed Asian country since at least 2021. The attackers used custom backdoors, including Coolclient, Quickheal, and Rainyday, to maintain prolonged access and steal sensitive credentials. They also expanded their reach to a supporting services company in the telecom sector and a university.

The tools and techniques used align with those of known Chinese threat actors. Apart from the custom backdoors, the attackers also used keylogging malware, port-scanning tools, and credential theft methods. Researchers have also provided indicators of compromise. Security professionals are advised to remain vigilant and adopt proactive defence strategies to stay safe against such threats.

ATTACK TYPE	Malware	SECTOR	Telecommunications
REGION	Asia	APPLICATION	Generic

Source - https://symantec-enterprise-blogs.security.com/threat-intelligence/telecoms-espionage-asia

INTRODUCTION | COIN-MINER ATTACKS WEB SERVER | MALVERTISING CAMPAIGN SPREADS BACKDOOR | ONNX STORE TARGETS MICROSOFT 365 | VOID ARACHNE TARGETS VPN USERS | HIJACK LOADER ATTACKS USERS | MARKOPOLO TARGETS CRYPTO USERS | CYBERCRIMINALS EXPLOIT QR CODES | ATTACKERS EXPLOIT ZERO-DAY FLAWS | NEW DIAMORPHINE LINUX VARIANT EMERGES | ESPIONAGE CAMPAIGN TARGETS TELCOS

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.