TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 22, 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.

Vilsa Stealer malware targets browsers, wallets, and more

Researchers have discovered a new infostealer malware, Vilsa Stealer, with its source code published on GitHub. Notably, Vilsa's user-friendly interface lowers the technical barrier, making it accessible even to individuals with minimal PC knowledge. The malware primarily targets web browsers, collecting sensitive data such as login credentials, passwords, and cryptocurrency wallet information, including MetaMask. Additionally, it gathers credentials from messaging apps like Telegram, Steam, and Discord. While these functions are common among infostealers, Vilsa stands out due to its speed, reliability, and advanced stealth techniques, including obfuscation and heavy encryption, making it harder to detect.

Promoted primarily on Telegram, Vilsa's campaign uses risky channels given recent changes in data disclosure policies. The malware's reliance on encryption and lack of digital signatures complicates detection, making robust anti-malware solutions with AI-driven heuristic mechanisms essential for identifying and neutralising its threats. Despite its sophistication, proactive protection remains key to mitigating Vilsa Stealer's impact.

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

Source - https://gridinsoft.com/blogs/vilsa-stealer-malware/

New OilRig campaign targets entities in the Middle East

The Iranian threat actor, OilRig, also known as Earth Simnavaz (APT34, Crambus, Hazel Sandstorm), has been observed exploiting a patched Windows kernel vulnerability (CVE-2024-30088) in cyberespionage campaigns targeting the UAE and the Gulf region. This privilege escalation flaw, patched by Microsoft in June 2024, allows attackers to gain SYSTEM-level privileges by exploiting a race condition.

OilRig's tactics include deploying a custom backdoor, STEALHOOK, which exfiltrates credentials from on-premises Microsoft Exchange servers. The group initially gains access by infiltrating vulnerable web servers, dropping a web shell, and using the ngrok tool for persistence. Once inside, they abuse elevated privileges to drop the password filter DLL (psgfilter.dll), extracting sensitive credentials from domain controllers and local accounts. This advanced campaign highlights OilRig's ability to adapt its techniques, combining new vulnerabilities with tried-and-true methods for data theft and maintaining control over compromised networks.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Middle East, UAE	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/10/oilrig-exploits-windows-kernel-flaw-in.html

Crypto stealer rakes up 28,000 victims

A large-scale cryptocurrency-stealing malware campaign has impacted over 28,000 users in Russia, Turkey, Ukraine, and other Eurasian countries. Disguised as legitimate software, such as pirated office tools, game cheats, and trading bots, the malware is promoted through YouTube videos and fraudulent GitHub repositories. Victims are tricked into downloading password-protected archives that bypass antivirus scans. Once the password is entered, the archive extracts obfuscated scripts and DLL files that initiate the attack.

The malware disables Windows Recovery Services, hijacks legitimate system services, and modifies browser update processes to ensure persistence. Using Ncat, it establishes communication with a command-and-control (C2) server while exfiltrating system data, including security processes, via a Telegram bot. Though the full mining profits are unclear, researchers found that the malware's "clipper" had diverted $6,000 worth of cryptocurrency transactions. To avoid such threats, download software only from official sources and verify links shared on platforms like YouTube or GitHub.

ATTACK TYPE	Malware	**SECTOR**	Aviation, BFSI, construction, e-commerce, energy, government, healthcare, IT, mining, manufacturing, oil and gas, telecommunications
REGION	Global	**APPLICATION**	Windows

Source - https://www.bleepingcomputer.com/news/cryptocurrency/crypto-stealing-malware-campaign-infects-28-000-people/

BabyLockerKZ spreads across the world

Researchers have identified a new variant of the MedusaLocker ransomware, dubbed BabyLockerKZ, which has been active since late 2022. This ransomware has targeted over 100 organisations each month, causing widespread disruptions across Europe and South America. BabyLockerKZ, believed to be operated by a financially motivated threat actor (TA), possibly an Initial Access Broker (IAB) or ransomware affiliate, uses both publicly available tools and custom software to launch its attacks.

The group employs a unique “checker” tool for lateral movement, credential theft, and process monitoring, utilising Mimikatz and Remote Desktop Plus for automation. BabyLockerKZ evades detection by disabling antivirus and endpoint software, hiding malicious scripts in innocuous folders like “Music” and “Documents.” Despite similarities to MedusaLocker, BabyLockerKZ differs by storing encryption keys under “PAIDMEMES” in the Windows Registry, with unclear use in its Linux version. The group’s growing global reach underscores its sophisticated, opportunistic nature.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	South America, Europe	**APPLICATION**	Windows

Source - https://securityonline.info/new-medusalocker-ransomware-variant-babylockerkz-targets-victims-globally/

User privacy under threat from Yunit Stealer

Yunit Stealer is a sophisticated malware targeting sensitive user data, particularly browser-stored credentials, cryptocurrency wallets, and system information. It uses advanced techniques to evade detection, such as registry modifications, scheduled tasks, and PowerShell-based Windows Defender exclusions, ensuring persistence on compromised systems. The malware exfiltrates stolen data via Telegram and Discord webhooks and targets specific geographies to evade detection in non-targeted areas.

Distributed through malicious links, JavaScript, and PowerShell payloads, Yunit Stealer extracts passwords, cookies, and credit card data from browser databases, while scanning for cryptocurrency wallets like Atomic and Exodus. It achieves persistence by auto-executing on system boot and hiding its presence through command line obfuscation and hidden execution techniques. Mitigating this threat requires user awareness, email filtering, updated antivirus definitions, and enforcing two-factor authentication (2FA). Regular patching and continuous log monitoring are crucial for detecting and defending against Yunit Stealer's evolving tactics.

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

Source - https://cybersecsentinel.com/new-infostealer-malware-yunit-stealer-targets-credentials-and-crypto/

Mozilla patches critical Firefox vulnerability

Mozilla has released an emergency security update for Firefox to address a critical use-after-free vulnerability, tracked as CVE-2024-9680, which is actively exploited in attacks. This flaw arises in the Animation timelines of Firefox's Web Animations API, where freed memory is improperly accessed, allowing malicious actors to execute arbitrary code. The vulnerability affects both the latest Firefox standard release and Extended Support Releases (ESR).

An attacker can exploit this flaw to gain code execution within the browser's content process. Mozilla has confirmed reports of this vulnerability being exploited in the wild. Users are urged to upgrade immediately to the following patched versions to mitigate risk: Firefox 131.0.2, Firefox ESR 115.16.1, and Firefox ESR 128.3.1. Given the active exploitation of the vulnerability and limited information on attack methods, prompt updates are crucial.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Mozilla Firefox

Source - https://www.bleepingcomputer.com/news/security/mozilla-fixes-firefox-zero-day-actively-exploited-in-attacks/

Fortinet RCE vulnerability exposed, exploited

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a critical alert regarding a remote code execution (RCE) vulnerability in Fortinet products, identified as CVE-2024-23113, which attackers are actively exploiting. This vulnerability, a format string issue, impacts several Fortinet offerings, including FortiOS, FortiPAM, FortiProxy, and FortiWeb. It stems from the use of an externally controlled format string in the fgfmd daemon, which manages authentication requests and keep-alive messages.

This flaw enables attackers to execute arbitrary code on unpatched devices through specially crafted requests. Rated 9.8 out of 10 on the CVSS scale, it poses severe risks to confidentiality, integrity, and availability. Fortinet has released patches for the vulnerability, urging users to upgrade to the following versions: FortiOS 7.4.3 or higher, FortiProxy 7.4.3 or higher, FortiPAM 1.2.1 or higher, and FortiWeb 7.4.3 or higher. CISA has also placed CVE-2024-23113 in its Known Exploited Vulnerabilities (KEV) catalogue, requiring U.S. federal agencies to patch their systems by October 30, 2024. Organisations are advised to act promptly to secure their systems against potential unauthorised access and data breaches.

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

Source - https://cybersecuritynews.com/fortinet-rce-vulnerability-exploited/

Russian government under attack from Awaken Likho

Russian government agencies and industrial enterprises are under attack by a cyber threat group, Awaken Likho, also known as Core Werewolf and PseudoGamaredon. Active since at least August 2021, the group has been targeting entities involved in critical infrastructure and defence sectors. According to Kaspersky, a campaign initiated in June 2024 continues to impact Russian organisations, utilising MeshCentral agents for remote access instead of the previously used UltraVNC module.

The attacks primarily involve spear-phishing campaigns where malicious executables are disguised as Microsoft Word or PDF documents using deceptive double extensions. Opening these files triggers the installation of UltraVNC, granting attackers full control over compromised systems. Another key tactic involves the use of self-extracting archives to covertly install remote access tools, all while displaying a decoy document to the victim. Core Werewolf's operations have also extended to military bases and weapons research facilities.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Russia	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/10/cyberattack-group-awaken-likho-targets.html

Malware targets gamers for cryptocurrency

Users searching for game cheats are being targeted by malware campaigns that use Lua-based loaders to establish persistence and deliver additional payloads on infected systems. These attacks, prevalent worldwide, exploit the popularity of Lua supplements within the gaming community. First documented in March 2024, the campaign takes advantage of GitHub's platform quirks to stage malicious payloads. In related campaigns, researchers discovered that attackers use the same method to deliver RedLine information stealer, hiding malware-bearing ZIP archives within legitimate Microsoft repositories.

Recently, researchers reported attacks targeting users searching for pirated software, distributing SilentCryptoMiner, an open-source cryptocurrency miner, via Telegram channels and YouTube. Some variants of this malware also engage in clipboard hijacking and other malicious activities. Most victims are in Russia, India, and other Eurasian countries.

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

Source - https://thehackernews.com/2024/10/gamers-tricked-into-downloading-lua.html

Microsoft discloses five zero-day vulnerabilities in October Patch Tuesday

Microsoft's October 2024 Patch Tuesday includes 118 security updates, addressing five publicly disclosed zero-day vulnerabilities, with two actively exploited. Among the updates are three critical RCE flaws.
Here's the breakdown by category:

- 28 Elevation of Privilege vulnerabilities
- 7 Security Feature Bypass vulnerabilities
- 43 Remote Code Execution vulnerabilities
- 6 Information Disclosure vulnerabilities
- 26 Denial of Service vulnerabilities
- 7 Spoofing vulnerabilities

The five zero-days include vulnerabilities in MSHTML Platform, Microsoft Management Console, and Winlogon, among others, affecting various Windows components.
Key zero-days addressed:

- **CVE-2024-43573** (MSHTML Spoofing)
- **CVE-2024-43572** (Management Console RCE)
- **CVE-2024-6197** (Curl RCE)
- **CVE-2024-20659** (Hyper-V Bypass)
- **CVE-2024-43583** (Winlogon Elevation)

The update does not cover three previously patched Edge vulnerabilities.

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

Source - https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2024-patch-tuesday-fixes-5-zero-days-118-flaws/

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