TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: NOVEMBER 26, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Amid a myriad of complex and challenging cybersecurity threats, today's individuals, businesses, as well as government entities are struggling to stay operationally secure. Preventing operational disruptions, financial losses, and reputational damage depends on the strengthening of digital defences to safeguard the integrity, confidentiality, and availability of business data.

Thankfully, our weekly Cyber Threat Intelligence (CTI) report helps them stay up to date on globally emerging threats. With our comprehensive advisory services, your IT assets are safeguarded from persistent risks. Harnessing the insights from our threat intelligence report will help you comprehensively enhance your organisational security posture for a more secure future.

Ymir ransomware emerges in an evolving cyber threat landscape

Researchers have uncovered the Ymir ransomware that was deployed shortly after systems were compromised by the RustyStealer malware. Ymir uses innovative memory management techniques to execute code in memory, bypassing traditional ransomware detection methods. Ymir was observed attacking a Colombian organisation by encrypting files using the ChaCha20 cypher, with the ability to target specific directories via customisable commands. The attack leveraged credentials stolen by RustyStealer and tools like Advanced IP Scanner and SystemBC scripts for data exfiltration and highlights a potential trend where threat actors bypass Ransomware-as-a-Service (RaaS) platforms to act independently.

Other than this, Black Basta ransomware operators use Microsoft Teams, QR codes, and social engineering to gain access, while other ransomware like Akira exploits unpatched SonicWall SSL VPNs. Ransomware incidents remain prevalent despite law enforcement efforts, with politically motivated groups like CyberVolk weaponising ransomware. American officials are urging cyber insurance firms to cease reimbursing ransom payments to disrupt this ecosystem.

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

Source - https://thehackernews.com/2024/11/new-ymir-ransomware-exploits-memory-for.html

North Korean hackers deploy RustDoor malware in cryptocurrency attacks

North Korean state-sponsored threat actors are leveraging LinkedIn to deliver the RustDoor malware in targeted social engineering campaigns against cryptocurrency and decentralised finance (DeFi) sectors. Disguising themselves as recruiters from legitimate companies like STON.fi, attackers trick victims into downloading booby-trapped Visual Studio projects. These contain second-stage payloads, such as “VisualStudioHelper” and “zsh_env,” which act as backdoors and persist on macOS devices.

The malware, tracked as RustDoor, uses Objective-C and exploits its presence on a victim’s system to harvest sensitive information and maintain command-and-control (C2) communication through separate servers.

These campaigns also involve coding challenges and requests to execute unknown scripts, targeting company-owned devices. Such tactics align with previous North Korean operations like Operation Dream Job. Security researchers emphasise training employees to identify social engineering schemes, especially in industries susceptible to North Korea’s cyber campaigns, which are increasingly sophisticated and tailored to bypass detection.

ATTACK TYPE	Malware	**SECTOR**	BFSI
REGION	Global	**APPLICATION**	macOS

Source - https://thehackernews.com/2024/09/north-korean-hackers-target.html

New macOS backdoor potentially linked to ransomware

Researchers have identified a new macOS backdoor, the Trojan.MAC.RustDoor, which is believed to be linked to the BlackCat/ALPHV ransomware family that historically targets Windows systems. The malware is written in the Rust programming language and masquerades as an update for the Visual Studio code editor. Over at least three months, RustDoor has been extracting data from macOS Desktop, Documents, and user Notes folders, compressing the information into a ZIP file before sending it to a C2 server. Researchers have observed multiple backdoor variants and found indicators of compromise (IoCs) suggesting ties to ransomware campaigns, including the BlackBasta and BlackCat/ALPHV groups.

Notably, three of RustDoor's four C2 servers have been linked to prior ransomware operations targeting Windows environments, and its use of Rust aligns with the coding choice of ALPHV. The discovery is concerning and underscores the expansion of ransomware threats beyond Windows to macOS systems.

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

Source - https://www.darkreading.com/threat-intelligence/macos-targeted-by-new-backdoor-linked-to-alphv-ransomware

Remcos RAT variant delivered via an advanced phishing campaign

Fortinet's FortiGuard Labs has uncovered a sophisticated phishing campaign exploiting a new variant of Remcos RAT. The malware is delivered via phishing emails with malicious Excel attachments and exploits the CVE-2017-0199 vulnerability to execute code remotely. Opening the Excel file triggers the download of an HTA file, which then executes a malicious payload (dllhost.exe). The malware also employs process hollowing, injecting malicious code into a new process (Vaccinerende.exe) to remain undetected. Persistence is achieved by creating auto-run registry entries and ensuring reactivation after system reboots. The Remcos payload operates entirely in memory, avoiding traditional detection methods.

Once active, Remcos RAT connects to a C2 server, gathering system data and executing commands such as keylogging, screenshot capture, and process control. Advanced anti-analysis techniques, including dynamic API calls and anti-debugging mechanisms, enhance its stealth. Fortinet emphasises the need for robust defences to counter these evolving threats.

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

Source - https://securityonline.info/researcher-uncovers-new-phishing-campaign-deploying-remcos-rat-with-advanced-evasion-techniques/

Lazarus group explores code smuggling with custom extended attributes

APT Lazarus has introduced an innovative technique for concealing malicious codes by using custom extended attributes on macOS systems. Extended attributes and a metadata system for storing non-standard file information offer a new avenue for malware authors to hide their payloads. This technique parallels earlier methods, such as Bundlore adware's 2020 exploitation of macOS resource forks, which were previously used to store structured data but have since been deprecated. Moreover, Group-IB researchers have identified a new macOS trojan, dubbed RustyAttr, developed using the Tauri framework and initially signed with a leaked certificate. The malware remains fully undetected on VirusTotal, signalling a highly stealthy threat.

The findings attribute this activity to the Lazarus group with moderate confidence and suggest the group may be experimenting with code-smuggling techniques. The new method is not yet documented in the MITRE ATT&CK framework, underscoring its novelty and the need for vigilance against evolving threats.

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

Source - https://www.group-ib.com/blog/stealthy-attributes-of-apt-lazarus/

Russia-linked threat actor exploits NTLM zero-day flaw in cyberattacks

A zero-day vulnerability in Windows NT LAN Manager (NTLM), tracked as CVE-2024-43451 (CVSS 6.5), was exploited by a suspected Russian-linked group to target Ukraine. The vulnerability was discovered by ClearSky and patched by Microsoft. It enables NTLMv2 hash disclosure through minimal user interaction with malicious URL files, such as right-clicking or dragging. The attack chain involves phishing emails sent from a compromised Ukrainian government server, urging recipients to download academic certificates. Users interacting with the malicious URL file unknowingly trigger connections to a remote server, initiating the download of further payload including the open-source Spark RAT malware. The vulnerability also facilitates Pass-the-Hash attacks via the SMB protocol, granting attackers unauthorised access without passwords.

Ukraine's CERT-UA attributed the activity to the threat actor UAC-0194, while separately warning about financially motivated phishing campaigns targeting accountants and enterprises using remote banking systems. The campaigns underscore escalating cyber threats tied to geopolitical tensions.

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

Source - https://thehackernews.com/2024/11/russian-hackers-exploit-new-ntlm-flaw.html

Operation Cobalt Whisper targets key industries in Hong Kong and Pakistan

SEQRITE Labs APT-Team has uncovered Operation Cobalt Whisper, a targeted cyberespionage campaign affecting industries like defence, energy, civil aviation, and academia. The campaign is primarily focused on Hong Kong and Pakistan and utilises the post-exploitation tool Cobalt Strike deployed via obfuscated VBScript. The campaign begins with malicious RAR archives containing decoy files, such as PDF and LNK documents, which execute scripts like O365.vbs. These scripts decode and activate a Cobalt Strike implant – cache.bak – enabling in-memory execution and communication with a C2 server. Over 20 infection chains and 30 decoy files have been identified so far, with 90% of attacks targeting Hong Kong-based researchers.

Industries impacted range from environmental engineering to medical research, underscoring the campaign's breadth. The use of sophisticated TTPs – malicious LNK files and VBScript-based payloads – illustrates an advanced, persistent effort to compromise sensitive sectors, highlighting significant cybersecurity risks in the targeted regions.

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

Source - https://www.seqrite.com/blog/operation-cobalt-whisper-targets-industries-hong-kong-pakistan/

G700 RAT targets Android devices and cryptocurrency applications

Researchers have identified G700 RAT, an evolved variant of Craxs RAT, as a significant threat targeting Android devices and cryptocurrency applications. Built on C# for desktops and Java for Android, this advanced malware exploits security gaps to perform privilege escalation, intercept sensitive data, and hijack cryptocurrency transactions. Its key features include bypassing authentication mechanisms, intercepting OTPs via SMS, and injecting fake banking or cryptocurrency app interfaces to steal credentials. The malware also manipulates cryptocurrency transactions by redirecting funds through counterfeit platforms. With extensive permissions, it gains access to SMS, contacts, and device storage, posing a critical risk to applications like Trust Wallet.

Distributed via dark web forums and Telegram channels, G700 RAT uses phishing, malicious APK distribution, and persistent obfuscation techniques to remain undetected. The persistent and evasive nature of G700 RAT underscores the need for robust security measures and heightened awareness to counter its expanding threat.

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

Source - https://www.cyfirma.com/research/g700-the-next-generation-of-craxs-rat/

Advanced campaign leveraging multi-stage infection chain

Researchers have uncovered a sophisticated campaign utilising a multi-stage PowerShell infection chain to establish persistence, bypass defences, and potentially facilitate advanced attacks using the Chisel tool. The attack begins with a malicious LNK file that activates a remote, obfuscated PowerShell script. This first stage sets up persistence and deploys a secondary PowerShell script and batch files while the second-stage script maintains communication with the C2 server, downloading and executing a third-stage PowerShell script. This final script requests and executes command chains from the C2 server, enabling malicious activities like data exfiltration and lateral movement.

An analysis of the campaign's infrastructure revealed a Chisel DLL, suggesting its use for setting up a SOCKS proxy and enabling stealthy C2 communications. The campaign also leverages the Netskope proxy for C2 traffic, highlighting the threat actor's advanced methods and focus on persistence and evasion.

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

Source - https://cyble.com/blog/dissecting-a-multi-stage-powershell-campaign-using-chisel/

TATA COMMUNICATIONS

BrazenBamboo exploits Fortinet zero-day vulnerability to steal VPN credentials

BrazenBamboo, a sophisticated threat actor, has been exploiting a zero-day vulnerability in Fortinet's FortiClient for Windows to extract VPN credentials using a modular framework called DEEPDATA. Identified in July 2024, DEEPDATA operates as a multi-stage post-exploitation tool leveraging DLLs to deploy plugins for credential theft, data exfiltration, and surveillance. A key feature is its ability to target communication platforms like WhatsApp, Signal, and Telegram, capturing sensitive data stealthily.

The malware portfolio also includes DEEPPOST for advanced data theft and LightSpy, a versatile tool targeting Windows, macOS, and iOS systems. The tools share infrastructural overlaps, suggesting development by a centralised Chinese organisation. LightSpy, with plugins for remote commands and data collection, exemplifies the group's advanced cyberespionage capabilities. Despite reporting the Fortinet flaw in July, the vulnerability remains unpatched, emphasising the urgent need for enhanced cybersecurity to counter these advanced threats.

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

Source - https://thehackernews.com/2024/11/warning-deepdata-malware-exploiting.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

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.

© 2024 Tata Communications. All rights reserved. TATA COMMUNICATIONS and TATA are trademarks of Tata Sons Private Limited.