TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: SEPTEMBER 10, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

As the digital realm gets more dynamic, cyber threats have become a serious concern to organisations worldwide. Since these threats are always changing, businesses attempt to not only secure their information but also safeguard the various IT frameworks that constitute contemporary operations. It is about the ability to protect against a range of new risks.

Improve your organisation's readiness against cyber threats with Tata Communications' weekly threat intelligence advisory. Gain valuable insights on current cyber risks to plan and implement effective measures to strengthen your cybersecurity.

Malware infiltrates messaging apps

Security experts have uncovered a macOS version of backdoor malware HZ RAT targeting the users of Chinese messaging platforms such as DingTalk and WeChat. Upon installation, the malware HZ RAT initiates communication with a command-and-control server, enabling attackers to issue commands and obtain sensitive information about users. Although the Windows version of HZ RAT has been active since 2020, this new adaptation to macOS clearly shows that the cybercriminals behind it are continuously refining their tactics.

Experts are yet to determine how widespread this campaign is. They warn that although the malware is currently used only to collect user data, it may be used later to spread across the victim's network causing more damage than just data theft.

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

Source - https://thehackernews.com/2024/08/macos-version-of-hz-rat-backdoor.html

Atlassian Confluence vulnerability exploited

Cybersecurity researchers have warned against broad cryptojacking efforts that exploit a serious vulnerability (CVE-2023-22527) in the Atlassian Confluence Data Center and Server. This vulnerability enables attackers to access devices and install cryptocurrency mining malware, effectively stealing computational resources. Since June 2024, the number of attempts to exploit this vulnerability has been on the rise, hurting enterprises worldwide. The malware degrades system performance and raises operational costs, as hijacked systems are misused to mine cryptocurrency.

Organisations using Atlassian Confluence are strongly encouraged to implement robust security measures immediately to protect against this ongoing threat. These include network segmentation, installation of endpoint detection and response solutions, and conducting regular security audits to assess vulnerability.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Atlassian Confluence

Source - https://securityonline.info/cryptojacking-campaign-exploits-atlassian-confluence-cve-2023-22527-vulnerability/

Angry Stealer malware targets sensitive data

A sophisticated dropper binary is being actively promoted on online platforms such as Telegram. This binary is used to deploy an infostealer malware dubbed "Angry Stealer," which poses a significant threat to consumers globally. The malware can steal credentials, browser information, cryptocurrency wallets, and VPN credentials. The Angry Stealer malware shares identical code, behaviour, and functionality with “Rage Stealer” malware. Angry Stealer offers advanced features, such as securely circumventing SSL validations and transmitting sensitive data to a remote server without being noticed.

The emergence of Angry Stealer indicates the constantly changing threat landscape, in which cybercriminals use increasingly complex tactics to infiltrate systems. Organisations must implement robust cybersecurity measures such as regular upgrades, strong encryption, and vigilant monitoring for odd activity to ensure that their sensitive information is not compromised.

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

Source - https://www.cyfirma.com/research/a-comprehensive-analysis-of-angry-stealer-rage-stealer-in-a-new-disguise/

TATA COMMUNICATIONS

Versa Director flaw exploited to harvest credentials

The China-linked Volt Typhoon group is being implicated in an advanced cyberespionage campaign exploiting a zero-day vulnerability (CVE-2024-39717) in Versa Director. The flaw enables cybercriminals with administrator privileges to upload malicious files camouflaged as PNG image. The malicious files included a customised web shell called VersaMem designed to intercept and harvest credentials, which are used to enable further supply chain attacks. The attack targeted Internet service providers and managed service providers in the IT sector, mainly from the United States.

Cybersecurity experts urge organisations using Versa Director to immediately upgrade to version 22.1.4 or later. Volt Typhoon's continued activity highlights the persistent threat posed by state-linked cyberespionage outfits.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic, Versa networks

Source - https://thehackernews.com/2024/08/chinese-volt-typhoon-exploits-versa.html

BlackByte exploits VMware vulnerability

The BlackByte ransomware group is exploiting a recently patched vulnerability (CVE-2024-37085) in VMware ESXi hypervisors. Exploiting vulnerable drivers, the group bypasses security mechanisms and spreads ransomware over networks. Tactics that BlackByte has used over time include double extortion and self-spreading ransomware for more efficient wide-scale attacks. This evolution of the methods they use testifies to the adaptability of the group and the serious, continuous menace it has posed to global cybersecurity.

Cybersecurity experts have urged organisations that use VMware ESXi to apply the latest updates and assess their security procedures. The BlackByte group's tenacity and innovation highlight the vital need for comprehensive and proactive cybersecurity tactics to combat growing threats.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, construction, IT, transportation, education
REGION	Global	**APPLICATION**	VMWare ESXi

Source - https://thehackernews.com/2024/08/blackbyte-ransomware-exploits-vmware.html

Malware threatens Gmail users

Cyber threat researchers have uncovered a malware named MalAgent.AutoITBot that targets Gmail users. The malware, complied using AutoIT, is obfuscated with advanced techniques and anti-debugging mechanisms. Once activated, it captures keystrokes, reads clipboard data, and controls system inputs. MalAgent.AutoITBot poses a formidable threat because of its capability of information theft and manipulation, which might let it gain unauthorised access to personal and corporate accounts. Such smartly designed malware outsmarts traditional security measures and makes cases of data breaches more probable.

The threat highlights the importance of strong cybersecurity practices. Experts suggest using strong, regularly updated passwords and implementing multifactor authentication. Users are warned to be vigilant, monitor their accounts for suspicious activities, and ensure that their systems are updated with the latest protection against this emerging threat.

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

Source - https://securityonline.info/sonicwall-warns-new-malware-targets-gmail/#google_vignette

PEAKLIGHT downloader targets Windows

Cybersecurity researchers have spotted PEAKLIGHT, a new type of in-memory dropper that attacks Windows systems. It is distributed through the supply chain by fake pirated movie downloads. PEAKLIGHT executes a PowerShell-based downloader that installs various malware strains, including Lumma Stealer and CryptBot. This dropper uses sophisticated evasion techniques to remain undetected. The dropper executes its payload entirely in memory and leaves behind minimal traces, further complicating detection and removal efforts.

Users are urged to download files only from trusted, legitimate sources. Organisations and individuals should make their cybersecurity defences stronger to mitigate such sophisticated attacks.

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

Source - https://thehackernews.com/2024/08/new-peaklight-dropper-deployed-in.html

Tickler backdoors critical networks

A new backdoor malware, named Tickler, has been unleashed by APT33, or Peach Sandstorm, an Iranian state-sponsored hacking group. They have used it to threaten several critical sectors across the United States, including government, defence, and oil industries between April and July 2024. These attacks targeted password spray and infiltrated Azure infrastructure to compromise these networks. The malware allowed APT33 to gain persistent access, jeopardising national security. Advanced techniques resorted to by APT33 show the persistence of danger against focused cyber-attacks on vital infrastructures.

To counter these attacks, Microsoft has made multifactor authentication mandatory for all Azure sign-in attempts starting October 15. Organisations in highly regulated sectors are advised to revisit their defences to ensure all systems are tightened in anticipation of such highly sophisticated attacks.

ATTACK TYPE	Vulnerability	**SECTOR**	Government, oil and gas, defence
REGION	United Arab Emirates, United States	**APPLICATION**	Windows

Source - https://www.bleepingcomputer.com/news/security/APT33-Iranian-hacking-group-uses-new-tickler-malware-to-backdoor-us-govt-defense-orgs/

APT-C-60 exploits zero-day in WPS Office

The APT-C-60 cyberespionage gang used a zero-day vulnerability, CVE-2024-7262, in the Windows version of WPS Office to deploy the SpyGlace backdoor on enterprise targets in East Asia. APT-C-60 embedded malicious hyperlinks hidden under a decoy image in spreadsheet documents (MHTML files) to trick the victims into clicking them, activating the exploit. The flaw allowed attackers to infiltrate systems and conduct espionage. Kingsoft, the developer of WPS Office, silently patched the issue in March 2024 without notifying users, leaving millions vulnerable.

An additional vulnerability, CVE-2024-7263, has also been discovered which Kingsoft patched in late May 2024. Security experts explain that this vulnerability can be exploited locally or through a network share, where the malicious DLL could be hosted. Users of WPS Office are advised to update to the latest release immediately, or at least 12.2.0.17119, to address both code execution flaws.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	East Asia	**APPLICATION**	WPS Office

Source - https://www.bleepingcomputer.com/news/security/apt-c-60-hackers-exploited-wps-office-zero-day-to-deploy-spyglace-malware/

New Snake Keylogger variant spreads

Researchers have discovered a new phishing campaign that delivers a new variant of Snake Keylogger, a potent .NET-based malware, via a malicious Excel document. The Excel file contains a specially crafted embedded link object that exploits the CVE-2017-0199 vulnerability to download a malicious file. The vulnerability is used to run multi-layered, disguised payloads that give the malware the ability to steal sensitive information, such as credentials and system data while avoiding detection. The stolen data is then sent to the attacker using the SMTP protocol. This variant is particularly dangerous because it uses advanced obfuscation techniques that allow bypassing traditional security measures, possibly increasing the risk of data breaches.

The unveiling of this campaign underlines how far advanced cybercrooks have been in their capability to compromise systems and exfiltrate data. Therefore, organisations and individuals should be wary of unsolicited e-mail attachments and maintain up-to-date cybersecurity practices. Snake Keylogger is always evolving, necessitating an alert with new methods to protect against such growing dangers.

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

Source - https://www.fortinet.com/blog/threat-research/deep-analysis-of-snake-keylogger-new-variant

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