TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: April 30, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Cyber threats expose businesses to data breaches, operational disruptions, and reputational damage. Partnering with cybersecurity experts can enable enterprises to identify vulnerabilities, implement advanced defences, and respond to attacks swiftly. Every organisation, regardless of size or industry, must prioritise security measures to thrive.

Stay ahead of cyber threats with Tata Communications' weekly threat intelligence report. Subscribe to our report to get actionable insights into emerging cyber risks and build strong defences.

Wiper malware expands from Linux to Windows

Discovered in October 2023, amid the Israel-Hamas conflict, the “BiBi” wiper malware, originally tailored for Linux systems, has now morphed to exploit Windows platforms through phishing tactics and compromised websites. Diverging from typical ransomware, its latest version, CrossBlur_1.15.4_AE.exe, causes irreversible data destruction by incapacitating system recovery and manipulating boot settings.

Beyond corrupting most files and sparing only those with .exe, .dll, and .sys extensions, the malware erases shadow copies, impeding file restoration. Remarkably, it shares a multithreading capability with its Linux counterpart, amplifying its prowess in executing concurrent processes. This poses formidable challenges for cybersecurity experts engaged in combatting its proliferation. As the threat landscape continues to evolve, vigilance and proactive security measures are imperative to mitigate the impact of such sophisticated cyber threats.

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

Source- https://app.cloudsek.com/gti/Z2xvYmFsX3RocmVhdF9pbnRlbF92MiM0dEMyNVk0QktJRHlfaHQ3dTN1Mw?org=2646

Malware-triggered vulnerability scanning surges

Researchers have observed a growing preference among cybercriminals for malware-based scanning attacks over direct methods. This strategic shift enables them to conceal their identities, harness resources from compromised hosts, and evade geographical restrictions, thereby heightening the complexity of detection efforts. An analysis of multi-network traffic logs reveals a significant transition in scanning behaviours toward compromised hosts for malicious intents.

These findings emphasise the urgent requirement for robust patch management practices and the deployment of updated detection systems to effectively combat the evolving threat landscape driven by emerging scanning techniques. Proactive measures in this regard are indispensable to fortify defences, thwart potential intrusions, and safeguard critical assets against the persistent and evolving tactics employed by cyber adversaries.

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

Source- https://unit42.paloaltonetworks.com/malware-initiated-scanning-attacks/

Brute-force attacks target VPNs and SSH services

Cisco has issued a critical advisory regarding a significant uptick in VPN and SSH assault incidents worldwide, commencing on March 18, 2024, heightening concerns over unauthorised network breaches and potential service interruptions. Malicious actors have been utilising brute-force techniques and anonymity tools such as TOR and proxies to obfuscate their identities, posing grave risks to major VPN services like Cisco Secure Firewall VPN and Checkpoint VPN.

The broad targeting of both generic and organisation-specific usernames suggests a systematic and indiscriminate attack approach. Given the dynamic nature of the source IP addresses associated with these assaults, organisations must maintain continuous vigilance and implement customised security protocols to safeguard affected services effectively.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Checkpoint VPN, Cisco VPN, Fortinet VPN, SonicWall Global VPN Client

Source- https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/

Botnets continue targeting TP-Link vulnerability

In 2023, cybersecurity researchers discovered a critical vulnerability, CVE-2023-1389, affecting TP-Link Archer AX21 routers, rendering them vulnerable to unauthenticated remote code execution (RCE) attacks. Despite attempts to patch the flaw, malicious botnets such as AGoent, Miori, Moobot, and a Gafgyt variant persist in exploiting unremedied systems to orchestrate distributed-denial-of-service (DDoS) attacks and propagate malware.

This vulnerability, prevalent in TP-Link Archer AX21 routers running version 1.1.4 Build 20230219 or earlier, permits remote attackers to assume control over compromised systems, posing a severe risk. Despite mitigation efforts, the threat landscape remains active, underscoring the critical need for proactive defence measures, ongoing updates, and diligent system monitoring to safeguard against potential breaches and mitigate the impact of cyberattacks.

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

Source- https://www.fortinet.com/blog/threat-research/botnets-continue-exploiting-cve-2023-1389-for-wide-scale-spread

Cybercrime group strikes enterprises with SteganoAmor campaign

Security analysts have recently uncovered the “SteganoAmor” campaign, orchestrated by the cybercriminal group TA558, which has set its sights on the hospitality and tourism sectors across Latin America, unleashing over 320 documented assaults. This insidious campaign utilises steganography to covertly embed malware within images and text files, with threats like Agent Tesla and FormBook disseminated via phishing emails adorned with romantically titled attachments. To enhance the credibility of their phishing schemes, the group leverages compromised SMTP and FTP servers.

These attacks exploit the CVE-2017-11882 vulnerability found in Microsoft Office Equation Editor. Upgrading to a newer version of Microsoft Office is imperative to mitigate these risks and bolster defences against such sophisticated cyber threats, safeguarding crucial data and organizational integrity from potential compromise.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Latin America	**APPLICATION**	Windows

Source- https://www.bleepingcomputer.com/news/security/new-steganoamor-attacks-use-steganography-to-target-320-orgs-globally/

Threat actor group FIN7 spear-phishes automotive giant

The notorious cybercrime syndicate, FIN7 recently launched a sophisticated spear-phishing campaign against a leading American automotive manufacturer, specifically targeting IT personnel. The attackers aimed to implant the Arunak backdoor by duping high-privilege individuals into clicking on malicious URLs disguised as legitimate software tools. Despite the intricate nature of the assault, involving multiple stages encompassing deceptive domains and malware, the company's robust security protocols thwarted the attack, preventing it from advancing beyond initial system compromise.

To fortify defences against such formidable threats, businesses must prioritise comprehensive security measures. This includes implementing multi-factor authentication (MFA), conducting regular employee training programs, and adhering to baseline security practices such as routine software updates and vigilant network monitoring. Such proactive measures are indispensable in safeguarding against increasingly sophisticated cyberattacks.

ATTACK TYPE	Malware	**SECTOR**	Automobile, manufacturing
REGION	US	**APPLICATION**	Windows

Source- https://www.bleepingcomputer.com/news/security/fin7-targets-american-automakers-it-staff-in-phishing-attacks/

TATA COMMUNICATIONS

APT group Sandworm uses Kapeka malware for espionage

A Finnish cybersecurity entity has recently uncovered Kapeka, a highly sophisticated malware suspected to have links with the Russia-affiliated APT group, Sandworm. This malicious tool is specifically targeting Eastern European countries, with a focus on nations like Estonia and Ukraine. Functioning as an advanced backdoor toolkit, Kapeka facilitates initial network infiltration and maintains prolonged operations within compromised systems. Its intricate two-stage attack process involves utilising a self-deleting dropper to activate the backdoor, cleverly disguised as a Microsoft Word add-in.

Microsoft has also identified Kapeka, also known as KnuckleTouch, in several ransomware campaigns. Capable of executing a multitude of malicious functions, including data theft and remote access provisioning, Kapeka poses a severe threat to cybersecurity. Its utilisation of dynamic command-and-control (C2) updates and sophisticated evasion techniques heightens the risk of APT-level cyber intrusions, underscoring the critical need for robust defence mechanisms and proactive cybersecurity measures.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Eastern Europe	**APPLICATION**	Windows

Source- https://thehackernews.com/2024/04/russian-apt-deploys-new-kapeka-backdoor.html

Ransomware exploits Atlassian server vulnerability

Exploiting the CVE-2023-22518 security loophole in Atlassian Confluence Data Center servers, cyber attackers have been deploying a Linux variant of the Cerber ransomware. This vulnerability allows assailants to reset configurations and establish administrator accounts, thereby gaining full control to execute the ransomware.

Financially motivated cybercriminal factions are leveraging these newly created admin credentials to install the Effluence web shell plugin, enabling the remote execution of arbitrary commands. Notably, the utilisation of pure C++ payloads in these attacks, amidst the proliferation of new ransomware strains targeting Windows and VMware ESXi servers, underscores the critical importance of regular software updates and bolstered security protocols. Proactive measures in this regard are imperative to mitigate the escalating risk posed by cyber threats and safeguard organisational assets from potential compromise.

ATTACK TYPE	Ransomware, vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Atlassian Confluence

Source- https://thehackernews.com/2024/04/critical-atlassian-flaw-exploited-to.html

TATA COMMUNICATIONS

Hackers exploit Fortinet vulnerability with a new campaign

Fortinet FortiClient EMS devices have become the focal point of the Connect:fun cyberattack campaign, leveraging the SQL injection vulnerability CVE-2023-48788. Initially discovered following an assault on an undisclosed media company, this campaign utilises ScreenConnect and Metasploit Powerfun payloads to retain control over compromised systems. By leveraging meticulously crafted requests, threat actors exploit the vulnerability to execute unauthorised codes and commands.

Researchers have been closely monitoring this campaign, emphasising the critical need for prompt implementation of security patches provided by Fortinet and enhanced monitoring protocols. This incident underscores the ever-present threat posed by cyberattacks and highlights the essential role of proactive security measures in mitigating potential risks and safeguarding against unauthorised intrusions.

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

Source- https://thehackernews.com/2024/04/hackers-exploit-fortinet-flaw-deploy.html

Cybercriminals target governments with Lazy Stealer malware

In early 2024, the cybercriminal syndicate dubbed “Lazy Koala” launched a series of targeted assaults on government bodies spanning Russia, Belarus, Kazakhstan, and other nations in Central Asia. Employing the deceptively uncomplicated yet highly effective malware “LazyStealer,” the attackers executed basic phishing schemes to pilfer credentials, resulting in the compromise of over 800 accounts. Upon analysis, cybersecurity experts discovered a commonality among all samples of the malware – they utilised PyInstaller as a packer, with the underlying code further obscured by Pyarmor.

Decompiling the code unveiled the utilisation of DLLs compiled with Cython, which were activated upon import. Despite its apparent simplicity, the malware’s robust protection mechanisms facilitated the seamless exfiltration of data, which was subsequently transmitted to Telegram bots. The widespread geographical scope of this campaign, coupled with its significant impact on governmental entities, underscores the urgent necessity for fortified cybersecurity measures and heightened vigilance to combat emerging threats effectively.

ATTACK TYPE	Malware
REGION	Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan
SECTOR	Healthcare/hospitals, government, education, BFSI
APPLICATION	Generic

Source- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/lazystealer-sophisticated-does-not-mean-better/

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