TATA COMMUNICATIONS

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 23RD, 2024

TATA COMMUNICATIONS

TATA

# THREAT INTELLIGENCE ADVISORY REPORT

In the ever-evolving landscape of digital progress, individuals, businesses, and governmental entities are constantly grappling with complex cybersecurity threats. These challenges have the potential to disrupt routine operations and entail significant financial repercussions. So, it is imperative to fortify your digital defences and shield your organisation from cyber threats that pose risks to the integrity, confidentiality, and availability of enterprise data.

Elevate your security protocols by integrating our weekly reports, delivering the latest cyber threat intelligence. Safeguard your IT assets against malicious attacks with our all-encompassing advisory services. In an age where cyber resilience holds paramount importance, our cyber threat intelligence report empowers your organisation with crucial knowledge to enhance its security stance.

# Syrian hackers distribute Silver RAT to fuel cybercrime wave

Anonymous Arabic, a Syrian hacking group, has released the stealthy Silver remote access trojan (RAT) malware. The treat actor (TA) offers various cybercriminal services like cracked RATs and fake bots, highlighting their diverse threat presence. Silver RAT boasts of advanced features like remote control, keylogging, and even ransomware, with versions for both Windows and Android planned.

Crafted in C#, it possesses the ability to elude antivirus measures. It clandestinely initiates concealed applications, browsers, and various other malicious activities. When creating a payload using the Silver RAT builder, malicious actors have the flexibility to choose from various options, allowing a payload size of up to 50kb. Upon connection, the targeted individual becomes visible on the Silver RAT panel controlled by the attacker, showcasing logs corresponding to the selected functionalities. The TA can obscure processes under misleading headings, and the ultimate payload is formed into a Windows executable file, distributed through diverse social engineering methods. Researchers have identified one member and noted their activity across social media, forums, and development platforms, confirming their broad malware distribution network.

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

Source - https://www.cyfirma.com/outofband/a-gamer-turned-malware-developer-diving-into-silverrat-and-its-syrian-roots/

# Turkish threat actors target Dutch ISPs and telcos

The Sea Turtle, a cyberespionage group linked to Turkey, has expanded its operations to the Netherlands. It is targeting sectors such as telecommunications, media, internet service providers (ISPs), and Kurdish websites.

Using techniques like domain name system (DNS) hijacking and traffic redirection, the group focuses on gathering economic and political intelligence aligned with Turkish interests. Sea Turtle's operational strategy includes intercepting internet traffic aimed at targeted websites. It can potentially grant unauthorised access to government networks and other organisational systems. The incorporation of a reverse shell mechanism in their operations facilitates the efficient collection and extraction of sensitive data, advancing their agenda. Despite moderate sophistication, Sea Turtle poses a significant threat worldwide, emphasising the need for stringent network monitoring, multi-factor authentication, and minimising secure socket shell (SSH) exposure.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware, cyberespionage | **SECTOR** | IT, broadcast media production and distribution, IT services and consulting, telecommunications |
| **REGION** | Netherlands | **APPLICATION** | Linux |

Source - https://www.huntandhackett.com/blog/turkish-espionage-campaigns

# New macOS backdoor SpectralBlur linked to North Korean hackers

Researchers have uncovered a new macOS backdoor called SpectralBlur. The backdoor is associated with North Korean TAs and shares similarities with KANDYKORN. This reveals a growing trend of North Korean cyber threats targeting macOS, with a focus on high-value entities in the cryptocurrency and blockchain sectors.

SpectralBlur can upload/download files, execute a shell, modify its configuration, erase files, hibernate, or sleep. These actions are carried out based on commands received from its command-and-control (C2) server. It utilises “grantpt” to establish a pseudo-terminal and execute shell commands received from the C2 server. The sophisticated malware, exhibiting file manipulation and stealth capabilities, underscores the evolving tactics of TAs. 21 new macOS-targeted malware families were identified in 2023, indicating a rising threat landscape.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Global | APPLICATION | Apple macOS |

Source - https://thehackernews.com/2024/01/spectralblur-new-macos-backdoor-threat.html

# Cracked software promoters on YouTube spreading Lumma stealer malware

TAs are leveraging YouTube videos featuring cracked software content to distribute Lumma, an information-stealing malware. Lumma is designed to target sensitive information encompassing user credentials, system particulars, browser data, and extensions. Its presence has been promoted on the dark web and a Telegram channel since 2022, featuring over a dozen observed C2 servers in the wild, along with multiple updates.

The YouTube videos used by Lumma commonly showcase content associated with pirated applications, offering users installation guides alongside the inclusion of malicious URLs frequently shortened using services like TinyURL and Cuttly. In a strategic move to bypass conventional web filter blacklists, the attackers leverage open-source platforms such as GitHub and MediaFire instead of establishing their own malicious servers. By enticing users seeking pirated software, particularly video editing tools, attackers deliver payloads that can exploit compromised machines for data theft and illicit mining. This tactic is part of a broader trend involving various malware. It coincides with warnings about stream-jacking attacks on YouTube and other phishing campaigns targeting high-profile accounts.

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

Source - https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

# Multi-stage malware masquerades as New Year greeting

New Year-themed spam emails containing a ZIP file named “happy new year.zip” are posing a malware threat. The emails include a ZIP attachment with a shortcut file camouflaged as a portable network graphics (PNG) image.

The disguised PNG file triggers MSHTA (designed to execute Windows script host code embedded within HTML) to download and display a harmless image. Behind the scenes, the JavaScript covertly retrieves and decodes a harmful payload through the Certutil executable, involving a cabinet (CAB) file. Following extraction, this CAB file releases the malware executable. Upon activation of the malware executable, it deploys a subsequent stage dynamic link library (DLL) payload. It utilises DLL sideloading to advance the infection and establish a connection with its C2 server, a potential Remcos RAT server. This highlights the evolving sophistication of attackers exploiting themed emails and urges caution around festive seasons.

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

Source - https://cyble.com/blog/festive-facade-dissecting-multi-stage-malware-in-new-year-themed-lure/

# Microsoft SQL servers hit by Mimic ransomware gang

A financially driven Turkish hacker collective, conducting operations under the alias RE#TURGENCE, is systematically focusing on Microsoft structured query language (SQL) servers on a global scale. It is using the Mimic ransomware to target the servers. The examined threat campaign concludes through one of two outcomes: either selling “access” to the compromised host or ultimately delivering ransomware payloads.

The TAs successfully employ brute force to infiltrate the victim server, utilising the xp_cmdshell procedure to execute commands on the host. Normally, this procedure is disabled by default. It should not stay enabled, particularly on servers exposed to the public. In this instance, the TA is deploying Cobalt Strike payloads, and infiltrating networks to unleash Mimic ransomware, with connections to the Phobos ransomware group. This follows a similar Microsoft SQL (MSSQL) server targeting campaign called DB#JAMMER last year, indicating a persistent threat.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Ransomware | **SECTOR** | All |
| **REGION** | Europe and the United States | **APPLICATION** | Microsoft SQL Server |

Source - https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-returgence-attack-campaign-turkish-hackers-target-mssql-servers-to-deliver-domain-wide-mimic-ransomware/

TATA COMMUNICATIONS

# Water Curupira group deploys PikaBot loader malware in a new spam campaign

Water Curupira, a TA group, has been actively spreading the PikaBot loader malware through phishing campaigns since 2023. Following the takedown of QakBot in August last year, PikaBot has emerged as its replacement. The operators of PikaBot orchestrated phishing campaigns, aiming at victims through its dual components - an initial loader and a central module. These components facilitated illicit remote access, enabling the execution of arbitrary commands through an established connection with their C2 server.

The malware is utilising email thread hijacking techniques with ZIP attachments to initiate its execution sequence. Functioning primarily as a loader, PikaBot is engineered to initiate another payload. The attack chains exploit ongoing email conversations to deceive recipients into opening malicious links or attachments. This method effectively triggers the execution sequence of the malware. The end goal is to deploy Cobalt Strike and activate the Black Basta ransomware, with a strategic shift towards an exclusive focus on PikaBot in recent activities.

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

Source - https://thehackernews.com/2024/01/alert-water-curupira-hackers-actively.html

# New botnet hijacks servers for secret digging

In 2023, a novel crypto-mining botnet named NoaBot surfaced. It was developed on Mirai code. Distinguished by obfuscation, custom mining pool utilisation, and an emphasis on non-default passwords for lateral movement, NoaBot showcases distinctive features. It carries a self-spreading worm and an SSH key backdoor, allowing it to download and execute additional binaries or extend its reach to new victims. Although rooted in Mirai, NoaBot's spreader module utilises an SSH scanner to identify servers vulnerable to dictionary attacks. It then employs brute-force techniques to add an SSH public key to the .ssh/authorised_keys file for remote access. After successful exploitation, it can download and execute additional binaries or propagate itself to new victims.

NoaBot is potentially linked to another botnet using P2PInfect malware. Researchers have identified approximately 850 infected IPs, primarily concentrated in China. Effective mitigation strategies encompass limiting public SSH access and enforcing the use of robust passwords.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Linux |

Source - https://thehackernews.com/2024/01/noabot-latest-mirai-based-botnet.html

# Malvertising campaign distributes new Atomic Stealer variant

In a late 2023 update, Atomic Stealer has incorporated payload encryption as a measure to evade detection. Atomic Stealer is a well-known Mac malware. In the realm of criminal underground activities, this stealer has gained notable popularity, with its developers consistently incorporating new features to substantiate the substantial monthly rental fee of $3,000.

In December, the TA initiated a promotional offer through their Telegram channel, providing a special holiday discount to its clientele. Around December 17, modifications were made to Atomic Stealer's code. It aimed to conceal specific strings that were previously utilised for the detection and identification of its C2 server. On January 8, a malvertising campaign was detected, employing tactics reminiscent of TAs distributing FakeBat. In this particular instance, an updated version of Atomic Stealer included a payload designed for Mac users. The TAs enticed victims through a Google search ad, posing as Slack – a popular communication tool. The victims were directed to a decoy website. There, they could download the app, which was supposedly designed for both Windows and Mac systems. Users are urged to download software only from trusted sources and use web protection/antivirus tools to stay safe.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Malware | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | Apple macOS |

Source - https://www.malwarebytes.com/blog/threat-intelligence/2024/01/atomic-stealer-rings-in-the-new-year-with-updated-version

# Over 150,000 WordPress sites at risk due to vulnerable plugin

Two critical vulnerabilities have been identified in the widely used post simple mail transfer protocol (SMTP) mailer WordPress plugin. Tracked as CVE-2023-6875 and CVE-2023-7027, they affect versions up to 2.8.7.

CVE-2023-6875 is a critical authorisation bypass vulnerability stemming from a “type juggling” issue within the connect-app representational state transfer endpoint. The second vulnerability is a cross-site scripting (XSS) issue, denoted as CVE-2023-7027, resulting from inadequate input sanitisation and output escaping. Exploiting these flaws allows attackers to manipulate authentication, reset application programming interface (API) keys, and potentially gain administrator privileges. A patch, version 2.8.8, has been released. However, an estimated 150,000 sites still run vulnerable versions, emphasising the urgency of updating to mitigate potential risks.

| | | | |
|---|---|---|---|
| **ATTACK TYPE** | Vulnerability | **SECTOR** | All |
| **REGION** | Global | **APPLICATION** | WordPress |

Source - https://www.bleepingcomputer.com/news/security/over-150k-wordpress-sites-at-takeover-risk-via-vulnerable-plugin/

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*