TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 16TH, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the dynamic realm of digital advancements, individuals, businesses, and governmental bodies are constantly confronted with complex cybersecurity threats and challenges. These issues can potentially disrupt regular operations and carry significant financial consequences. So, it is crucial to strengthen your digital defences and protect your organisation against cyber threats that could compromise the integrity, confidentiality, and availability of enterprise data.

Enhance your security measures by following our weekly reports that provide the latest cyber threat intelligence. Safeguard your IT assets from malicious attacks with our comprehensive advisory services. In an era where cyber resilience is of utmost importance, our cyber threat intelligence report empowers your organisation with vital knowledge to elevate its security posture.

8base: The latest ransomware threat

8base is a ransomware variant driven by financial motives. It is believed to be rooted in the Phobos ransomware. The ransomware's delivery mechanism involves SmokeLoader variants carrying 8base, with its impact extending across various industry verticals.

Utilising a sophisticated encryption process, the ransomware specifically targets designated files, terminates processes, and employs advanced encryption standards (AES). Upon execution, the ransomware actively seeks files for encryption, excluding those within the cache folder. Furthermore, the 8base ransomware employs a file size check, establishing a threshold of 1.5 MB. Files smaller than this threshold undergo complete encryption, while larger files experience partial encryption, possibly to expedite the encryption process. A newer variant, coded in C, has introduced changes that include an extended ransom note and the integration of a data leak site utilising TOR or the open-source Onion Router technology. These changes underscore the dynamic and evolving nature of the threat.

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

Source - https://www.fortinet.com/blog/threat-research/ransomware-roundup-8base

A new variant of Bandook RAT utilises PDF and process injection

The Bandook malware, a persistent remote access trojan (RAT) has recently surfaced with a new variant. Researchers have provided a detailed account of its behaviour, highlighting modifications such as streamlined control codes, advanced injection techniques, and novel features in command and control (C2) communication.

The malware is being distributed via a PDF file. Within this PDF file lies a condensed URL. When accessed, the URL initiates the download of a password protected .7z file. Upon extraction using the password embedded in the PDF, the malware proceeds to inject its payload into the msinfo32.exe application. The payload is limited to accommodating 139 actions. Furthermore, certain distinctive commands are exclusively transmitted to the server when specific conditions are met. The malware's multifaceted capabilities include file manipulation, execution of commands, and control over the victim's computer environment, showcasing a sophisticated and continually developing threat landscape.

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

Source - https://www.fortinet.com/blog/threat-research/bandook-persistent-threat-that-keeps-evolving

New Chameleon Android trojan variant outwits fingerprint locks

The new Chameleon Android trojan variant is using Zombinder, a darknet platform, for distribution. Demonstrating its versatility, Chameleon reveals a range of novel commands, notably involving the scrutiny of app package names. It is also bypassing biometric checks.

The trojan primarily sets its sights on mobile banking applications, utilising phishing pages that masquerade as authentic apps for distribution. What sets this banking trojan apart is its unique ability to exert control over a victim's device, performing actions on its behalf through a proxy feature. This feature facilitates sophisticated including account takeover (ATO) and device takeover (DTO) attacks. In 61 countries, 29 recently identified or actively circulating malware families have aimed at compromising 1,800 banking apps. Fintech and trading apps are being targeted by these malicious activities. These attacks are specifically aimed at banking applications and cryptocurrency services and their capabilities hinge on the exploitation of accessibility service privileges.

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

Source - https://www.threatfabric.com/blogs/android-banking-trojan-chameleon-is-back-in-action

New malware wave spreads OCEANMAP, MASEPIE, STEELHOOK

The Computer Emergency Response Team of Ukraine (CERT-UA) has issued a warning about a phishing campaign by the APT28 group. The TA is targeting Ukrainian government entities and Polish organisations. The APT28 group, affiliated with Russia, has also been linked to exploiting a recently patched security flaw in Outlook. The malware allows unauthorised access to victims' accounts on Exchange servers.

The threat actor (TA) prompts recipients to click on a link in emails. It exploits JavaScript and the "search-ms:" URI protocol handler, dropping a Windows shortcut file (LNK). This activates an infection chain for a new Python-based malware called MASEPIE, allowing file operations and command executions over an encrypted transmission control protocol (TCP) channel to its C2 server. The attacks have introduced additional malware, including STEELHOOK, a PowerShell script that harvests web browser data. Another component is OCEANMAP, a C#-based backdoor that executes commands via cmd.exe.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Poland and Ukraine	**APPLICATION**	Windows

Source - https://thehackernews.com/2023/12/cert-ua-uncovers-new-malware-wave.html

North Korean hackers unleash an arsenal of backdoors in new attacks

North Korean hackers, linked to Kimsuky APT, are installing the backdoors such as AppleSeed, Meterpreter, and TinyNuke for espionage. The TA conducts espionage campaigns through spear-phishing attacks, employing malicious lure documents. Upon opening, these documents lead to the deployment of various malware families.

The Windows-based backdoor employed by Kimsuky is AppleSeed (aka JamBog). It is a dynamic link library (DLL) malware being utilised since at least May 2019. The backdoor has undergone updates, including an Android version and a new Golang variant called AlphaSeed. AppleSeed operates by receiving instructions from an actor-controlled server, dropping additional payloads, and exfiltrating sensitive data such as files, keystrokes, and screenshots. Kimsuky also deploys Meterpreter, virtual network computing (VNC) malware, and TinyNuke for remote control. These attacks highlight North Korea's evolving cybercrime tactics and economic motives.

ATTACK TYPE	Information gathering and malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://thehackernews.com/2023/12/kimsuky-hackers-deploying-appleseed.html

Unveiling qBit stealer: Source code leak raises exfiltration concerns

The qBit ransomware-as-a-service (RaaS) group has introduced a recently developed ransomware, coded in Go. On October 9, 2023, the qBit team also presented the qBit stealer, developed using the Go language, emphasising its claim of being undetectable by endpoint detection and response (EDR) solutions.

This stealer excels in efficiently uploading any file to Mega[.]nz, employing an advanced concurrency engine for swift uploads. It is available for purchase, with a trial version accessible. On December 5, 2023, the qBit stealer's source code was announced to be distributed freely. Upon analysing the source code, researchers identified a unique trait in qBit. It selectively focuses on files with specific extensions. This distinct feature suggests its potential application as an exfiltration tool in ransomware operations. With the stealer now accessible at no cost, there is an increased risk of its adoption by numerous new, less sophisticated TAs.

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

Source - https://cyble.com/blog/decoding-qbit-stealers-source-release-and-data-exfiltration-prowess/

CISA warns of active attacks targeting Chrome and Excel parsing library

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two recently discovered flaws to its known exploited vulnerabilities (KEV) catalogue. They have been identified as CVE-2023-7024 in Google Chrome's WebRTC and CVE-2023-7101 in Spreadsheet::ParseExcel.

The Spreadsheet::ParseExcel flaw can enable remote code executions (RCE). The vulnerability arises from the unvalidated input passed from a file into a string-type "eval." More precisely, the problem originates from the evaluation of number format strings within the Excel parsing logic. The flaw was exploited by Chinese hackers targeting Barracuda Email Security Gateway in late December. The CVE-2023-7024 issue, on the other hand, is a heap buffer overflow in WebRTC within the Google Chrome web browser. Google Chromium WebRTC is an open-source initiative that furnishes web browsers with real-time communication capabilities. This vulnerability enables an attacker to instigate crashes or execute malicious codes. Federal agencies need to attend to these security issues by January 23.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Google Chrome OS

Source - https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-bugs-in-chrome-and-excel-parsing-library/

New phishing wave targets Ukrainian entities with Remcos RAT

UAC-0050, a cyber threat entity, is employing advanced phishing tactics to distribute Remcos, a RAT. The group has been persistently targeting Ukraine and Poland since 2020, employing deceptive campaigns and evolving techniques to compromise specific geopolitical regions. The Remcos RAT, a well-known malware recognised for remote surveillance and control, stands as a prominent element in their espionage toolkit.

In their most recent operational activities, the UAC-0050 group has incorporated a pipe method for inter-process communication, highlighting their advanced adaptability. The trojan has been disseminated in various phishing waves. In one particular attack, it also facilitated the deployment of an information stealer named Meduza Stealer. This underscores the critical necessity of meticulously scrutinising links obtained from unverified or suspicious sources. Staying well-informed about potential threats remains crucial.

ATTACK TYPE	Phishing and malware	**SECTOR**	Government
REGION	Ukraine	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/01/uac-0050-group-using-new-phishing.html

Critical flaw detected in Ivanti EPM software

Ivanti has fixed a critical RCE vulnerability in its endpoint management (EPM) software. It can allow attackers to take control of devices or the core server. Tracked as CVE-2023-39366, the flaw impacts all versions of Ivanti EPM that are currently supported.

Ivanti EPM facilitates the management of client devices operating on diverse platforms, including Windows, macOS, Chrome OS, and various IoT operating systems. In scenarios where attackers gain access to a target's internal network, they can exploit this vulnerability through low-complexity attacks that do not require privileges or user interaction. Upon exploitation, an attacker within the internal network can utilise an unspecified structured query language (SQL) injection to execute arbitrary SQL queries, extracting output without requiring authentication. The company has released version 2022 Service Update 5 to address the issue, emphasising that no customer instances were affected. This follows earlier incidents in July involving zero-day vulnerabilities in Ivanti's endpoint manager mobile (EMM).

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

Source - https://www.bleepingcomputer.com/news/security/ivanti-warns-critical-epm-bug-lets-hackers-hijack-enrolled-devices/

Corrupt PyPI packages: Cryptocurrency miner executed on Linux systems

Three malicious packages have been discovered in the Python package index (PyPI). Referred to as modularseven, driftme, and catme, they installed a cryptocurrency miner on Linux devices. All three packages are crafted by an individual identified as “sastra.” They come from the same source. The creator had set up a PyPI account shortly before uploading the initial malicious package. Collectively, they had amassed 431 downloads before being taken down.

Similar to the “culturestreak” campaign, the packages utilise remote URLs. They hide their payload and employ multi-stage releases to evade detection. The initiation of malicious activity occurs through the “import” statement within an init.py file. The malware introduces a novel element by adding malicious commands to the ~/.bashrc file, ensuring persistent and stealthy exploitation of the victim’s device. In this specific package set, malicious actors consistently enhance their tactics to obscure and prolong the exploitation process. So, the ability to recognise subtle malicious indicators is of utmost importance.

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

Source - https://www.fortinet.com/blog/threat-research/malicious-pypi-packages-deploy-coinminer-on-linux-devices

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