TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 6TH, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the dynamic realm of digital advancements, individuals, businesses, and government entities are constantly grappling with complex cybersecurity challenges. These threats not only have the potential to disrupt daily operations but can also lead to significant financial repercussions. So, it becomes crucial to fortify your digital defences and shield your organisation from cyber threats that can compromise the integrity, confidentiality, and availability of vital enterprise data.

Take your security protocols to the next level by integrating our weekly reports, delivering cutting-edge insights in cyber threat intelligence. In an era where cyber resilience is a top priority, our cyber threat intelligence report equips your organisation with invaluable knowledge to elevate its security stance. Ensure the protection of your IT assets against malicious attacks through our comprehensive advisory services. Stay ahead of cyber threats.

Apple addresses the year's first zero-day vulnerability exploited in the wild

Apple has released security updates for various platforms, addressing a zero-day vulnerability. Identified as CVE-2024-23222, it pertains to a WebKit confusion flaw. This vulnerability could be leveraged by attackers to achieve code execution through web content manipulation.

Upon successful exploitation, threat actors (TAs) gain the capability to execute arbitrary malicious codes on devices operating susceptible versions of iOS, macOS, and tvOS. This occurs when users access a malicious web page. The range of devices impacted by this WebKit zero-day is extensive. CVE-2024-23222 has been resolved by Apple through enhanced checks in iOS 16.7.5 and subsequent versions, iPadOS 16.7.5 and later, macOS Monterey 12.7.3 and higher, and tvOS 17.3 and later. Although Apple acknowledged instances of real-world exploitation, specific details have not been disclosed.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apple macOS, Apple IOS, and Apple Safari

Source - https://www.bleepingcomputer.com/news/apple/apple-fixes-first-zero-day-bug-exploited-in-attacks-this-year/

Cracked macOS apps use DNS hijack method to steal crypto wallets

Hackers are employing a sophisticated technique to deploy information-stealing malware on macOS Ventura. The macOS malware family has been exploiting cracked software as a means of infiltration. The TAs focus exclusively on users utilising the latest operating system versions, spanning both Intel processors and Apple silicon machines.

The campaign hides bad scripts using domain name system (DNS) records to steal crypto wallets. To escalate their privileges, the TAs simply request the password during software installation, a move that often goes unnoticed by users and raises no suspicions. Users unknowingly download and run the malware when they use compromised apps, thinking they are activating something else. A programme named “Activator” is embedded alongside the desired application for installation. Upon opening or mounting the image, a window emerges, providing installation instructions. The attackers connect to a control server in a unique way through DNS, keeping their actions hidden in network traffic. This showcases the adaptability and sophistication of their approach.

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

Source - https://securelist.com/new-macos-backdoor-crypto-stealer/111778/

NS-STEALER malware targets popular browsers, uses Discord bots for data exfiltration

Cybersecurity experts have uncovered NS-STEALER, a sophisticated malware. It is a Java-based stealer disseminated through zip files containing cracked software. The malware utilises JDABuilder classes to create an instance of EventListener, an inbuilt JavaScript feature that awaits the occurrence of an event, to facilitate easy registration. It utilises a Discord bot channel as its EventListener.

The malware is compatible with specific browsers such as Chrome, Edge, and Opera. It actively searches for autofill credentials, which users commonly employ to save passwords. The usernames and passwords are extracted from the supported browser's “Login Data” folder using the query “select * from logins.” In another development, the Chaes malware has launched version 4.1, featuring an improved Chronod module. It is utilising email lures with legal themes in Portuguese. Interestingly, the source code of the malware includes expressions of gratitude towards a security researcher, indicating an uncommon interaction between TAs and the security community.

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

Source - https://www.trellix.com/about/newsroom/stories/research/java-based-sophisticated-stealer-using-discord-bot-as-eventlistener/

New wave of info-stealing packages discovered in PyPI

Researchers have uncovered a Python package index (PyPI) malware author operating under the alias “WS.” This individual clandestinely uploads malicious packages to PyPI that target Windows users.

PyPI functions as an open repository containing software packages created by the Python community. Its purpose is to facilitate the swift development of applications. The identified packages, namely nigpal, figflix, telerer, seGMM, fbdebug, sGMM, myGens, NewGends, and TestLibs111, include the base64-encoded source code of portable executable (PE) or other Python scripts within their setup.py files. Upon installation, depending on the victim device's operating system, these Python packages drop and execute the final malicious payload. They exfiltrate sensitive information, emphasising the need for users to exercise caution against evolving threats.

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

Source - https://www.fortinet.com/blog/threat-research/info-stealing-packages-hidden-in-pypi

New malware campaign targets asylum seekers in the US

A suspicious URL is distributing a malicious ZIP archive, targeting individuals interested in U.S. immigration through social engineering. The ZIP archive file is possibly accessible through a URL or distributed via spam emails.

The ZIP contains a deceptive shortcut LNK file (files with a . lnk extension) disguised as a PDF document. When this shortcut file is activated, it triggers a virtual private network (VPN) application that uses dynamic link library (DLL) sideloading to load a hidden malicious DLL. Both the VPN application and the DLL are concealed within the ZIP archive. The loaded DLL activates Microsoft Software Installer (MSI), which downloads the misleading PDF lure and presents it to the victim. Additionally, the DLL drops a Windows cabinet (CAB) file housing a malware stealer named “MetaStealer.” During the post-infection process, MetaStealer establishes a connection with the command-and-control (C2) server, enabling the unauthorised exfiltration of data.

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

Source - https://cyble.com/blog/threat-actors-target-us-asylum-seekers-with-metastealer-malware/

Trigona ransomware attackers using Mimic for enhanced file encryption

A Trigona ransomware campaign involving Mimic ransomware is targeting Microsoft structured query language (MS-SQL) servers. The modus operandi involves bulk copy programme (BCP)-assisted deployment, information gathering, credential theft, AnyDesk installation, and a dual strategy of encrypting systems and extracting sensitive information.

The command line tool, bcp.exe or the BCP utility, serves to import or export extensive external data from MS-SQL server. The assault targets insecure MS-SQL servers and systems exposed to external threats, making them susceptible to brute force or dictionary attacks by manipulating account information. This inference stems from the presence of infection logs indicating the deployment of malicious codes like LoveMiner and Remcos RAT. In this particular attack scenario, it is presumed that the attacker employed a technique involving the storage of malicious codes in the database, followed by their conversion into a local file using the BCP utility. Trigona, active since June 2022, replaced Mimic in a January 2024 attack. This suggests a connection between them, emphasising the need for enhanced security measures on MS-SQL servers.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	Global	**APPLICATION**	Microsoft SQL Server

Source - https://asec.ahnlab.com/ko/60744/

Parrot TDS exploits hacked sites with malicious scripts

Since October 2021, an ongoing campaign has been employing a traffic direction system (TDS) to target susceptible WordPress and Joomla sites. Identified as Parrot, the TDS has been discovered on at least 16,500 compromised websites. It capitalises on traffic through the sale of user data to TAs.

Websites utilising Parrot TDS are compromised with malicious scripts inserted into the pre-existing JavaScript code stored on the server. The injected script consists of an initial landing script for profiling the victim and a payload script capable of redirecting the victim's browser to a malicious destination or content. The identification of the Parrot TDS involves recognising specific keywords such as “Ndsj,” “Ndsw,” and “Ndsx” within the injected JavaScript. When the conditions specified by the landing script are met successfully, the victim's web browser initiates a query to a payload server. The payload server responds by delivering a JavaScript payload that includes the keywords. Despite continuous updates, the TDS remains an active and evolving threat. To address this, it is recommended that website owners regularly conduct server searches and scans.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Joomla and WordPress

Source - https://unit42.paloaltonetworks.com/parrot-tds-javascript-evolution-analysis/

TATA COMMUNICATIONS

BianLian ransomware targets the healthcare and manufacturing sectors of EU and the US

The BianLian ransomware group has been active since 2022. It is now targeting the healthcare and manufacturing sectors of Europe and the US. Recently, their approach has shifted from employing a double extortion scheme to one focused on extortion without encryption. Instead of encrypting the assets of their victims, followed by threatening to publish the data if the ransom is not paid, the attackers are now directly moving to data theft to force their victims into making ransom payments.

In January 2023, the TA asserted that they had successfully extracted 1.7 terabytes of data, encompassing personal information of both patients and employees, from a hospital located in California. The targeting of healthcare organisations raises concerns. It could potentially disrupt the daily operations of hospitals, posing a risk to the lives of patients. The TA employs diverse infiltration tactics, ranging from the use of stolen credentials to exploiting vulnerabilities such as ProxyShell. This showcases their adaptability in tactics, allowing them to maintain a significant presence in the cyber threat landscape. The BianLian and Makop ransomware groups are linked by a common, specialised tool, suggesting a potential association between them.

ATTACK TYPE	Ransomware	**SECTOR**	Healthcare and manufacturing
REGION	Europe, India, and the US	**APPLICATION**	Windows

Source - https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/?utm_source=digesto&utm_medium=email&mkt_tok=NTMxLU9DUy0wMTgAAAGQ1gvK-LWM8qVZY9pbX194G6tlUzPyt76k-hSZfzsO2N3frz0I9DZ4mJ0dY8UysCpKmjEwaI-SiGmXicOBv0twpcp4dtn5PYVJStGxJU_5DD6gug0bO5Q

New Kasseika ransomware uses driver to deactivate antivirus software

A newly identified ransomware, named “Kasseika,” has adopted the bring your own vulnerable driver (BYOVD) strategy to steal credentials. The ransomware disables antivirus software before encrypting files with ChaCha20 and Rivest, Shamir, Adleman (RSA) algorithms. Kasseika exploits the Martini driver known as Martini.sys/viragt64.sys, to disable antivirus products and compromise the security of targeted systems.

Linked to BlackMatter, the new ransomware starts with phishing emails to steal employee credentials for initial network access. Kasseika operators then use Windows PsExec, a lightweight telnet alternative designed for executing processes on remote systems, to run malicious .bat files on infected and other accessed systems. The batch file checks for “Martini.exe,” terminates it, and downloads the vulnerable “Martini.sys” driver on the compromised machine. Then the TA demands a ransom of 50 Bitcoins, which is $2,000,000, within 72 hours. The demand increases by $500,000 every 24 hours. Victims are required to share proof of payment in a private Telegram group to receive assistance with decryption.

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

Source - https://www.bleepingcomputer.com/news/security/kasseika-ransomware-uses-antivirus-driver-to-kill-other-antiviruses/

TATA COMMUNICATIONS

New Go-based CherryLoader malware exploits CherryTree app for privilege escalation

A recently identified malware loader named CherryLoader, built in Go language, has been discovered in the wild. It is being utilised to deploy additional payloads on compromised hosts. The loader disguises itself with the icon and name resembling the legitimate CherryTree note-taking application, aiming to deceive potential victims during the installation process.

CherryLoader poses a substantial threat by establishing persistence and disabling security tools. It is employed to deliver either PrintSpoofer or JuicyPotatoNG. Both serve as privilege escalation tools. These tools, in turn, execute a batch file, ensuring persistence on the victim's device. Adding a unique element, CherryLoader incorporates modularised features, enabling the TA to interchange exploits without recompiling the code. The malware leverages process ghosting to execute exploit files as separate logs, further enhancing its stealth.

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

Source - https://thehackernews.com/2024/01/new-cherryloader-malware-mimics.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