TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: JANUARY 9TH, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

In the ever-evolving digital landscape, individuals, businesses, and government entities are continually encountering intricate cybersecurity challenges. These risks pose a potential disruption to routine operations, leading to substantial financial repercussions. So, it is imperative to fortify your digital defences and shield them against cyber threats that may jeopardise the integrity, confidentiality, and availability of enterprise data.

Augment your security protocols by leveraging our weekly reports, offering the latest insights into cyber threat intelligence. Safeguard your IT assets from persistent threats through our comprehensive advisory services. In an era where cyber resilience holds paramount importance, our cyber threat intelligence report equips your organisation with the essential knowledge to enhance its security posture.

Iranian cyberespionage group targets African telcos with malware

MuddyWater, an Iranian cyberespionage group, is targeting telecommunications companies in Egypt, Sudan, and Tanzania. It is using a new Golang-based command-and-control (C2) framework called MuddyC2Go.

The threat actors (TAs) rely on phishing emails, unpatched vulnerabilities, and a mix of custom, living-off-the-land, and publicly available tools to evade detection and collect data. They leverage tools such as the SimpleHelp remote access tool and Venom Proxy, both previously linked to Seedworm activity. Additionally, they employ a bespoke keylogging tool and various publicly accessible and "living-off-the-land" tools. The initial signs of malicious actions were detected through PowerShell executions associated with the MuddyC2Go backdoor. A launcher for MuddyC2Go, identified as "vcruntime140.dll," was stored in the directory "csidl_common_appdata\javax." It appears that this launcher was sideloaded by jabswitch.exe, a legitimate executable for Java Platform SE 8. Meanwhile, the Israel-linked TA, Gonjeshke Darande, has initiated a cyber assault on Iranian gas pumps in retaliation to perceived Iranian aggression.

ATTACK TYPE	Malware	**SECTOR**	Telecommunications
REGION	Egypt, Sudan, and Tanzania	**APPLICATION**	Windows

Source - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-africa-telecoms

JaskaGO hits both Windows and Mac

The recently uncovered JaskaGO malware is posing a threat to both Windows and Apple macOS systems. It is utilising deceptive tactics and masquerading as legitimate software. The malware is built on the Go programming language. This aligns with a trend in malware development, leveraging Go's simplicity and cross-platform capabilities.

The malware demonstrates advanced capabilities, including manipulating the clipboard for cryptocurrency theft. It comes with a comprehensive set of commands received from its C2 server. JaskaGO performs checks to identify whether it is operating in a virtual machine (VM) environment. If detected, it carries out innocuous tasks such as pinging Google or printing a random number. This is a likely attempt to evade detection. In alternative situations, JaskaGO goes on to gather information from the targeted system and establishes a link to its C2 server to receive additional instructions. This includes tasks like executing shell commands, listing running processes, and downloading additional payloads.

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

Source - https://thehackernews.com/2023/12/new-go-based-jaskago-malware-targeting.html

FBI warns of Play ransomware outbreak targeting key organisations

The Play ransomware gang, implicated in infiltrating 300 organisations worldwide, has targeted critical infrastructure entities. This includes the City of Oakland, Arnold Clark, Rackspace, and the city of Antwerp. Employing unique tactics, the group exfiltrates sensitive data before deploying ransomware, using it to pressure victims. Ransomware affiliates associated with the Play choose email as their preferred channel for negotiations. They refrain from including Tor negotiation page links in the ransom notes left on compromised systems. Additionally, the gang employs a personalised volume shadow copy service (VSS) copying tool to pilfer files from shadow volume copies, even if those files are actively in use by applications.

The FBI and CISA of the United States and the Australian Signals Directorate's Australian Cyber Security Centre have issued a directive urging organisations to address vulnerabilities. Enterprises have been advised to implement multifactor authentication and adopt recommended mitigation measures to reduce the risk and impact of Play ransomware attacks.

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

Source - https://www.bleepingcomputer.com/news/security/fbi-play-ransomware-breached-300-victims-including-critical-orgs/

Rhadamanthys stealer grows more sophisticated

The Rhadamanthys information-stealing malware has undergone significant updates. Version 0.5.0 of the malware has introduced a modular plugin system for customisation.

Rhadamanthys, a C++ information-stealing programme, focuses on acquiring credentials for email, file transfer protocols (FTPs), and online banking services. This stealer follows a subscription model, being sold to cyber criminals, and its distribution to targets encompasses diverse channels such as malvertising, contaminated torrent downloads, emails, YouTube videos, and other means. In its most recent iteration, version 0.5.1, the software has improved capabilities. These enhancements include the integration of a clipper plugin for diverting cryptocurrency payments, options for exfiltrating wallet information through Telegram, the recovery of deleted Google account cookies, and the ability to evade detection by Windows Defender. This reflects the malware's rapid and dynamic evolution, likely attracting cybercriminals seeking a versatile tool for malicious activities.

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

Source - https://www.bleepingcomputer.com/news/security/rhadamanthys-stealer-malware-evolves-with-more-powerful-features/

Critical zero-day flaw in Chrome actively exploited

Google has released critical security updates for the Chrome web browser, addressing an actively exploited zero-day vulnerability in the WebRTC framework. Tracked as CVE-2023-7024, it poses the risk of crashes or arbitrary code executions. The vulnerability is characterised as a heap-based buffer overflow flaw within the WebRTC framework. As WebRTC is an open-source project and is also integrated into browsers like Mozilla Firefox and Apple Safari, the broader impact of this flaw remains uncertain, specifically outside of Chrome and Chromium-based browsers.

This marks the resolution of the eighth zero-day vulnerability in Chrome in 2023. Users are advised to update to Chrome version 120.0.6099.129/130 to mitigate potential risks, and users of Chromium-based browsers are urged to apply relevant fixes promptly for enhanced security. To prevent further abuse, no additional details about the security defect have been disclosed. However, Google has acknowledged the existence of an exploit for CVE-2023-7024 in the wild.

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

Source - https://thehackernews.com/2023/12/urgent-new-chrome-zero-day.html

New malvertising campaign distributes PikaBot malware

The PikaBot malware, associated with cyber threat actor group TA577, is now spreading through malvertising campaigns. It is targeting users seeking software like AnyDesk.

PikaBot acts as a backdoor and payload distributor, granting unauthorised remote access to compromised systems. Previously disseminated exclusively through malspam campaigns akin to QakBot, the malware has surfaced as a favoured payload for the TA TA577. The standard distribution process for PikaBot typically initiates with an email (thread hijacking), providing a link to an external website. Users are deceived into downloading a zip archive that harbours malicious JavaScript. The central module of PikaBot is injected into the SearchProtocolHost.exe process. Additionally, PikaBot's loader conceals its injection by employing indirect syscalls, making the malware highly stealthy. Furthermore, the rise in malvertising is showcased by the new loader HiroshimaNukes and the malicious Chrome extension ParaSiteSnatcher. This underscores the necessity for enhanced cybersecurity measures.

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

Source - https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads

8220 gang targets unpatched Oracle WebLogic servers with malware

The 8220 gang is exploiting a high-severity vulnerability in the Oracle WebLogic server. Identified as CVE-2020-14883, it enables remote code execution (RCE) and seizes control of vulnerable servers. Known for leveraging security flaws, the TA used this exploit along with CVE-2020-14882 to bypass authentication protocols. The 8220 gang is deploying stealer and coin-mining malware across various sectors and regions, showcasing an opportunistic and adaptable approach.

The 8220 gang employs two distinct gadget chains. One facilitates the loading of an extensible markup language (XML) file that, in turn, calls the other chain, allowing the execution of commands on the operating system. Various versions of the provided XML are used by the group depending on the target operating system. The TA seems to utilise custom Python tools for initiating their attack campaigns. The IPs involved in the attacks, situated in the United States, Mexico, and Russia, are linked to recognised hosting companies.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	Healthcare/hospitals, BFSI, and telecommunications
REGION	Colombia, Mexico, South Africa, Spain, and the United States	**APPLICATION**	Oracle WebLogic server

Source - https://www.imperva.com/blog/imperva-detects-undocumented-8220-gang-activities/

Hackers leverage GitHub to evade detection, control infected hosts

GitHub is being increasingly leveraged by cybercriminals for illicit purposes, such as hosting malware and conveying commands via concealed Gist and Git commit messages. The TAs deploy their samples on services such as Dropbox, Google Drive, OneDrive, and Discord to host second-stage malware, evading detection tools.

Researchers uncovered various Python package index (PyPI) packages, including httprequesthub, pyhttpproxifier, libsock, libproxy, and libsocks5. These posed as network proxy handling libraries. The packages, however, concealed a Base64-encoded URL directing to a secret Gist hosted on a disposable GitHub account devoid of any publicly visible projects. Consequently, the likelihood of an infected endpoint engaging with a GitHub repository being identified as suspicious is reduced. This transition complicates detection efforts, as these malicious activities seamlessly integrate with legitimate communications. The exploitation of GitHub Gists signifies a progression in this pattern. Gists, which are essentially repositories, provide a convenient means for developers to share code snippets.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	GitLab Community Edition (CE) and GitLab Enterprise Edition (EE)

Source - https://thehackernews.com/2023/12/hackers-abusing-github-to-evade.html

Cybercriminals impersonate UAE government in latest smishing wave

Smishing Triad, a Chinese cybercrime group, is masquerading as a UAE entity to steal personal data from residents and foreigners. The TA distributes malicious links to their targets' mobile devices via SMS or iMessage, employing URL-shortening services such as Bit.ly to obfuscate the links they transmit. They utilise compromised Apple iCloud accounts to spread smishing messages, aiming at identity theft and financial fraud. Smishing Triad offers smishing kits for $200 per month.

Their latest campaign targets visa holders and utilises geofencing to appear even more convincing. Individuals who click on the embedded link in the message are redirected to a fraudulent website (“rpjpapc[.]top”) mimicking the UAE Federal Authority for Identity, Citizenship, Customs, and Port Security (ICP). This deceptive site prompts users to input personal information, including names, passport numbers, mobile numbers, addresses, and card details.

ATTACK TYPE	Phishing	SECTOR	All
REGION	United Arab Emirates	APPLICATION	Generic

Source - https://thehackernews.com/2023/12/alert-chinese-hackers-pose-as-uae.html

Cyber threats ramp up for holidays, from Agent Tesla to Instagram phishing

Sophisticated phishing attacks are exploiting a Microsoft Office vulnerability (CVE-2017-11882) to disseminate the Agent Tesla malware. By employing decoy Excel invoices, cybercriminals trigger the vulnerability for potential code executions. The attackers strategically use terms like “orders” and “invoices” in spam emails, urging users to download malicious attachments containing CVE-2017-11882.

Another threat involves malware campaigns targeting the hospitality sector, employing information-stealing tactics. In these attacks, the TAs initiate contact through emails with minimal text, focusing on topics relevant to service-oriented businesses. After the target responds, they receive a follow-up email with a link supposedly containing details about their request or complaint. Additionally, a new Instagram phishing variant mimics Meta copyright infringement notifications, urging urgent appeal submissions within 12 hours to prevent permanent account deletion.

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

Source - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/instagram-phishing-targets-backup-codes/ | https://news.sophos.com/en-us/2023/12/19/inhospitality-malspam-campaign-targets-hotel-industry/ https://www.zscaler.com/blogs/security-research/threat-actors-exploit-cve-2017-11882-deliver-agent-tesla

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