TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: FEBRUARY 20TH, 2024

THREAT INTELLIGENCE ADVISORY REPORT

In the swiftly changing digital world, individuals, businesses, and governments encounter complex cybersecurity challenges daily. These threats can have critical consequences. They could compromise sensitive information, grant unauthorised access to confidential systems, disrupt business operations, incur significant financial losses, and cause irreparable harm to organisational reputation. Such scenarios ultimately lead to a loss of trust among stakeholders. So, it becomes imperative to fortify your company's digital barriers and shield against cyber threats endangering vital enterprise data.

Stay watchful against cyber perils. Elevate security by using our weekly briefings that offer cyber threat intelligence. Our threat intelligence dossier delivers invaluable insights to reinforce your organisation's security preparedness. Protect your IT assets from malevolent attacks through our comprehensive advisory solutions.

Cyberattack hits job listing websites, exposes data of two million users

ResumeLooters, a cyber threat group, has orchestrated a significant breach impacting over two million job seekers across the APAC region. It has infiltrated 65 reputable job listing and retail platforms through structured query language (SQL) injection and cross-site scripting (XSS) tactics. Their modus operandi involves exploiting vulnerabilities in legitimate websites, embedding malicious scripts to extract personal information, and selling stolen data for financial gain.

The threat actor (TA) has been named “ResumeLooters” due to its targeting of job search platforms and the theft of resumes. Employing SQL injection attacks on websites, the TA pilfers user databases containing names, phone numbers, emails, date of birth, and job seekers’ employment details. The stolen data is subsequently sold in Telegram channels. Traces of cross-site scripting (XSS) infection have also been discovered on legitimate job search websites. These scripts were designed to load further malicious scripts from related malicious infrastructure and present phishing forms on authentic platforms.

ATTACK TYPE	Breaches	SECTOR	HR and recruitment, real estate, investment management, and retailer and distributor
REGION	Russia, India, Brazil, Italy, Mexico, Taiwan, Thailand, Turkey, United States, and Vietnam	APPLICATION	Generic

Source - https://www.group-ib.com/blog/resumelooters/

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK’S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

Patchwork’s VajraSpy malware campaign using romance scams

Patchwork, a TA, is utilising romance scams to distribute the VajraSpy trojan on Android devices in India and Pakistan. With 12 espionage apps (including Rafaqat) identified, including six on Google Play, it has been downloaded over 1,400 times.

VajraSpy boasts of various espionage features that can be broadened according to the permissions assigned to the application bundled with its code. The malware steals contacts, files, call logs, and SMS messages. Moreover, certain implementations enable the extraction of WhatsApp and Signal messages and call recordings. It also captures images using the camera. This tactic mirrors past Patchwork operations, suggesting a link to Indian interests. Rafaqat stands out as the sole non-messaging app included in the list. The precise method of distributing the malware remains unclear. However, given the nature of the apps, it appears that targets were deceived into downloading them, likely as part of a honey-trap romance scam.

ATTACK TYPE	Malware	SECTOR	All
REGION	India and Pakistan	APPLICATION	Android

Source - https://thehackernews.com/2024/02/patchwork-using-romance-scam-lures-to.html

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK’S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

Revenge RAT malware operates in memory, stealing user data

A new strain of malware Revenge RAT has emerged recently. The malware operates in memory in a fileless fashion, gathering data from the user's PC and transmitting it to its command-and-control (C2) server in Base64-encoded format. It is disguised within a seemingly ordinary tool during distribution.

The TA employs tools like smtp-validator and "Email To Sms" during execution. At the same time, they create and run both legitimate tools and malicious files, complicating the user's ability to detect the malicious activity. Revenge RAT first creates and executes Setup.exe, a malicious file, before running smtp-verifier.exe, which is a legitimate tool. Subsequently, the file's attribute is modified to "Hidden," rendering it invisible in Windows Explorer under normal circumstances. This highlights the need for strong defences against sophisticated memory threats.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://asec.ahnlab.com/ko/61288/

New vulnerabilities discovered in FortiSIEM, Oracle WebLogic, and Apache Tomcat

Fortinet recently disclosed two critical vulnerabilities affecting the FortiSIEM supervisor, a cybersecurity solution aiding businesses in breach prevention, anomaly identification, and threat detection. These vulnerabilities, identified as CVE-2024-23108 and CVE-2024-23109, hold the maximum common vulnerability scoring system (CVSS) scores of 10.0 and involve operating system command injections.

The vulnerabilities stem from FortiSIEM's insufficient input sanitisation. It permits remote, unauthenticated TAs to manipulate application programming interface (API) requests. This manipulation could lead to the execution of unauthorised commands, unauthenticated data access, and potential data modification or deletion. Fortinet recommends updating to version 7.1.2 or higher. Additionally, Oracle's WebLogic server patch has resolved CVE-2024-20931, which could potentially expose close to three million instances. Versions 8.5.7 to 9.0.43 of Apache Tomcat have also been detected with the CVE-2024-21733 vulnerability. This flaw allows for unauthorised data smuggling. Users are urged to upgrade to secure versions.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Oracle WebLogic Server, Apache Tomcat, and Fortinet

Source - https://socradar.io/latest-vulnerabilities-in-fortisiem-oracle-weblogic-apache-tomcat/

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK'S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

Critical vulnerability in Shim bootloader impacts most Linux Distros

A critical flaw in the Shim Linux bootloader is allowing attackers to run codes and gain control of target systems before kernel loading, effectively bypassing current security measures. Shim is a compact open-source bootloader managed by Red Hat. It assists secure boot processes on systems utilising a unified extensible firmware interface (UEFI). The recent Shim vulnerability, identified as CVE-2023-40547, is located within the httpboot.c source code for Shim, utilised for booting network images via HTTP.

Shim version 15.8 has been released to address six security vulnerabilities, including CVE-2023-40547. Linux distributions have issued advisories, warning that the flaw stems from Shim's HTTP boot support, allowing for a fully controlled out-of-bounds write primitive. A remote attacker can conduct a man-in-the-middle (MiTM) attack. This allows them to intercept HTTP traffic intended for HTTP boot. The interception can occur from any network location situated between the victim and the server, emphasising the need for prompt updates and heightened security measures.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Canonical Ubuntu Linux, Debian Linux, Red Hat Enterprise Linux, SUSE Linux, and Linux

Source - https://www.bleepingcomputer.com/news/security/critical-flaw-in-shim-bootloader-impacts-major-linux-distros/

Chinese hackers lurk in US infrastructure for half a decade

It has been discovered that the Chinese cyberespionage group Volt Typhoon has successfully breached a critical infrastructure network in the United States and operated without detection for at least five years. Known for employing living-off-the-land (LOTL) tactics extensively, Volt Typhoon hackers utilise stolen accounts and implement robust operational security measures to evade detection and sustain prolonged access to compromised systems.

The joint advisory warns of Volt Typhoon's prolonged infiltration of U.S. critical infrastructure. Particularly concerning is their strategic shift towards targeting operational technology (OT) assets, raising fears of potential disruption to essential services during crises. The operatives engage in thorough pre-exploitation reconnaissance to understand the target organisation and its surroundings. They customise their tactics, techniques, and procedures (TTPs) to fit the victim's environment and allocate continuous resources to uphold persistence and control the target environment over time, even following the initial compromise. The authorities have issued alerts and provided technical guidance to fortify defences and mitigate such threats.

ATTACK TYPE	Malware and cyberespionage	SECTOR	Waste disposal, transportation, and energy
REGION	United States	APPLICATION	Windows

Source - https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK'S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

HijackLoader malware expands evasion techniques

The HijackLoader malware is evolving with new evasion tactics. Leveraged by cybercriminal groups like TA544, it is distributed through ClearFake and used in phishing campaigns to deploy various payloads. The malware developer employed a conventional process hollowing method alongside an extra trigger activated by the parent process writing to a pipe. This novel approach can enhance the stealthiness of defence evasion.

Utilising a sophisticated multistage attack process and advanced evasion techniques such as transacted hollowing and Heaven's Gate (a hook bypass method), HijackLoader is designed to circumvent conventional security measures. The initial phase of the multistage attack sequence begins with "client.exe" – an executable that verifies an active internet connection before retrieving a second-stage configuration from a remote server. Subsequently, the executable loads a genuine dynamic-link library (DLL) as defined in the configuration to trigger the shellcode responsible for deploying the HijackLoader payload.

ATTACK TYPE	Malware and cyberespionage	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://thehackernews.com/2024/02/hijackloader-evolves-researchers-decode.html

Fortinet warns of new critical SSL VPN vulnerability exploited in attacks

A critical vulnerability has been discovered in the FortiOS secure sockets layer (SSL) virtual private network (VPN). Tracked as CVE-2024-21762, the vulnerability has been assigned a severity rating of 9.6 on the CVSS scale. It constitutes an out-of-bounds write vulnerability within FortiOS, enabling unauthenticated attackers to achieve remote code execution (RCE) through maliciously crafted requests.

Fortinet's advisory lacks specifics regarding the exploitation method. Users should upgrade FortiOS versions as advised or disable SSL VPN if immediate patching is not feasible. Three other vulnerabilities, CVE-2024-23113, CVE-2023-44487, and CVE-2023-47537, have also been disclosed. This underscores the importance of timely updates to thwart potential cyber threats.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Fortinet

Source - https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/

Google Chromium bug added to CISA’s KEV list; ChromeOS and Edge also vulnerable

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added the CVE-2023-4762 bug to its known exploited vulnerability (KEV) list. The vulnerability affects versions of Google Chrome before 116.0.5845.179, enabling a remote attacker to execute arbitrary codes by utilising a crafted HTML page.

Additionally, researchers have found that Apple zero-days have been utilised to install the Cytrox Predator spyware, with one exploit chain including CVE-2023-4762. The TA possessed an exploit chain for installing Predator on Android devices within Egypt. The delivery of these exploits took place through the two distinct methods of MiTM injection and via one-time links sent directly to the target. Vulnerabilities found in Google ChromeOS and Microsoft Edge (Chromium-based) also pose risks of arbitrary code executions. Microsoft has issued the newest updates for the Microsoft Edge Stable Channel (Version 121.0.2277.112) and Microsoft Edge Extended Stable Channel (Version 120.0.2210.175), integrating the latest security updates from the Chromium project.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Microsoft Edge, Chromium, Google ChromeOS

Source - https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&amp;VLCODE=CIVN-2024-0031, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&amp;VLCODE=CIVN-2024-0030
https://securityaffairs.com/158820/security/cisa-adds-google-chromium-v8-type-confusion-bug-to-its-known-exploited-vulnerabilities-catalog.html?web_view=true

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK’S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

Hacktivist group accepts responsibility for cyberattacks targeting UAE, Bahrain

LulzSec Muslims have pledged allegiance to oppressed communities globally. The group, recognised for its past cyber operations targeting nations such as Israel and India, recently publicised the announcement through its X (formerly Twitter) account.

The TA has issued threats of cyberattacks on online infrastructure, as evidenced by a distributed denial of service (DDoS) attack on the Sharjah Airport. Additionally, they have admitted to hacking incidents, such as infiltrating a recruitment agency's database and compromising the data of 40,000 users. The group has issued a threat to target servers and websites associated with the United Arab Emirates and Bahrain, warning of cyberattacks on both nations aimed at disrupting their online infrastructure.

ATTACK TYPE	DDoS	**SECTOR**	Financial services
REGION	United Arab Emirates	**APPLICATION**	Generic

Source - Tata Communications

INTRODUCTION | JOB SITES BREACHED: USER DATA EXPOSED | PATCHWORK'S VAJRASPY ROMANCE CAMPAIGN | REVENGE RAT STEALS MEMORY DATA | NEW FLAWS IN FORTISIEM, ORACLE, TOMCAT | SHIM BOOTLOADER LINUX FLAW | CHINESE HACKERS INFILTRATE US | HIJACKLOADER BROADENS EVASION TACTICS | FORTINET ALERTS ON VPN FLAW | GOOGLE CHROMIUM ON CISA LIST | HACKTIVISTS TARGET UAE, BAHRAIN

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.