TATA COMMUNICATIONS

TATA

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: May 14, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

With increasing reliance on technology, cyber threats pose significant risks, including data breaches and operational disruptions. Partnering with cybersecurity experts is crucial for identifying vulnerabilities, implementing defences, and responding to attacks swiftly. Every organisation must prioritise security measures to thrive.

Keep cyber risks at bay with Tata Communications' weekly threat intelligence report. Subscribe for actionable insights on stronger defences.

DarkGate RAT executes AutoHotkey with HTML and XLS

A recent study sheds light on the sophisticated infection mechanisms of DarkGate malware, a Remote Access Trojan (RAT) traced back to 2018, now marketed as Malware-as-a-Service (MaaS) on a Russian cybercrime platform. The malicious software has multiple functionalities including process injection, file download and execution, data theft, shell command execution, and keylogging. Exploiting vulnerabilities like CVE-2023-36025 and CVE-2024-21412, DarkGate bypasses Microsoft Defender SmartScreen, using HTML and XLS files for malware distribution.

The infection chain begins with phishing HTML pages and Excel files, which trigger the execution of VBScript and PowerShell commands, ultimately deploying AutoHotkey to run malicious scripts. Analysis reveals the final payload as a Delphi-compiled executable, facilitating data theft and remote control. Users are urged to exercise caution, verify sender information, and maintain updated security software to mitigate such threats.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Australia, Canada, India, Japan, China, Germany, Indonesia, Italy, Malaysia, S. Africa, Spain, Turkey, U.S.	**APPLICATION**	Windows

Source- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-darkgate-menace-leveraging-autohotkey-attempt-to-evade-smartscreen/

TATA COMMUNICATIONS

Cuttlefish malware breaches routers and steals cloud credentials

A recently identified malware variant Cuttlefish has been targeting small office/home office (SOHO) routers since July 2023, stealing authentication details from HTTP requests passing through the routers. The malware presents a zero-click method for capturing data from users and devices within the targeted network's perimeter. Using advanced techniques such as DNS and HTTP hijacking, Cuttlefish targets IP addresses and has a secondary capability to interact with LAN-connected devices. The malware's ability to passively monitor network traffic with an eBPF and exploit stolen credentials as a proxy and a VPN poses a substantial risk.

Although Cuttlefish's code resembles the HiatusRat malware associated with Chinese interests, no shared victimology has been observed between the two. The infection pattern exhibits a distinct characteristic, with 99% of infections in Turkey, mainly from two telecommunications providers responsible for approximately 93% of infections, totalling 600 unique IP addresses. The small number of non-Turkish victims comprises IP addresses associated with likely clients of international satellite phone providers and a suspected US-based data centre. Users must remain vigilant and update router firmware to mitigate the risk.

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

Source- https://blog.lumen.com/eight-arms-to-hold-you-the-cuttlefish-malware/

Android malware Wpeeper targets compromised WordPress sites

Experts have uncovered a new Android malware strain Wpeeper which targets devices via compromised WordPress sites. The malware originated from altered applications within the UPtodown Store, where cyberattackers inserted a small code segment into standard APKs to deploy the malicious ELF. The slight addition of code makes the modified APKs undetectable on VirusTotal. Disguised within a fake UPtodown App Store app, Wpeeper acts as a backdoor Trojan, enabling data theft and remote control. With over 2,600 downloads, its complex command-and-control structure evaded detection until April 18, 2024.

Notably, Wpeeper uses encrypted communication, posing a challenge to detection. The malware abruptly ceased activity on April 22, 2024, and its downloaders and C2 servers stopped providing services. This unexpected halt suggests that a larger scheme may be in play. Wpeeper's stealthy tactics highlight the need for enhanced vigilance among Android users.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Android, WordPress

Source- https://blog.xlab.qianxin.com/playing-possum-whats-the-wpeeper-backdoor-up-to/

ViperSoftX uses Tesseract for data theft

Recent investigations have revealed that the ViperSoftX malware, initially detected in 2020, has evolved to employ the Tesseract OCR engine for extracting sensitive data from images on compromised systems. ViperSoftX spreads by presenting itself as a crack or keygen for genuine software, maintaining a continuous presence within compromised systems to implant additional malicious code. This sophisticated malware, which has evolved significantly since 2022, utilises methods like PowerShell scripts and malicious browser extensions to steal information, including cryptocurrency details.

Distributed through cracked software, ViperSoftX installs RAT and TesseractStealer malware to control infected systems and steal data. The malware's recent activities involve installing Quasar RAT, capable of remote control, and TesseractStealer, which extracts text from images. To avoid malware infection, users should download programs like utilities and games from official websites instead of suspicious websites or data-sharing sites. Other measures include updating V3 to the most recent version.

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

Source- https://asec.ahnlab.com/ko/64931/

TATA COMMUNICATIONS

ZLoader malware resurgence sparks cyber threat escalation

The comeback of ZLoader malware, a sophisticated version of the Zeus banking trojan, signals a concerning escalation in cyber threats. Also known as Terdot, DELoader, or Silent Night, ZLoader is a modular trojan rooted in the leaked 2015 ZeuS source code. Leveraging features designed to hinder analysis by restricting its activities to the initially infected device, modern cryptographic techniques, and enhanced domain generation algorithms, ZLoader poses extensive challenges to cybersecurity efforts. Using sophisticated tactics like black hat SEO, email-based phishing, and the deployment of additional malware, ZLoader's propagation is increasingly intricate.

Since its revival in September 2023, following a nearly two-year hiatus, ZLoader, now at version 2.4.1.0, has introduced measures to prevent execution on machines differing from the original infection, improving its stealth and resilience against detection and analysis. Reports indicate a targeted distribution strategy, prompting continued vigilance and detection updates from security providers.

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

Source- https://www.zscaler.com/blogs/security-research/zloader-learns-old-tricks

Pakistani APT groups launch AllaKore RAT (.NET) attacks on India

The cyber threat landscape in India is becoming increasingly sophisticated, with Pakistani APT groups such as SideCopy and APT36 targeting government and corporate sectors. These groups exploit advanced spear-phishing techniques, the dark web market for illegal access, and a surge in ransomware attacks. In the first quarter of 2024, Telegram-based hacker groups have carried out more than 2900 attacks, ranging from distributed denial-of-service (DDoS) attacks to website defacement and data breaches.

The advisory cements the need for advanced defence measures, exemplified by a case study on reverse-engineering the AllaKore RAT malware using DnSpy. This highlights the ongoing need for robust security measures and continuous cybersecurity education. Additionally, the advisory warns of emerging threats like RusticWeb and FlightNight spear-phishing campaigns and increased access to Indian entities on underground forums.

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

Source- https://medium.com/@pushpendrabharala7055/indian-government-on-alert-new-wave-of-cyberattacks-by-pakistani-groups-lets-reverse-engineer-6e5423e1bfb2

LightSpy malware variant targets macOS

A recent investigation into LightSpy malware exposes its impact on macOS devices, particularly those using Intel or Apple Silicon that support Rosetta 2, dispelling earlier assumptions linking it to iOS platforms. Researchers focused on the macOS variant, showcasing its extensive use of x86_64 architecture binaries, incompatible with iOS. LightSpy employs a dropper mechanism to deploy malicious plugins and sustains complex C2 communication over WebSockets, indicating sophisticated development and targeted functionalities for macOS.

The malware was initially misidentified as an iOS implant, whereas it targets macOS. The macOS version demonstrates refined operational security and development practices compared to its iOS counterpart. Although historically associated with APT 41, the specific target remains unconfirmed. Apple has introduced new security features like Lockdown Mode and TCC restrictions to counter such threats, emphasising the importance of regular device updates for user protection.

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

Source- https://www.huntress.com/blog/lightspy-malware-variant-targeting-macos

Cybercriminals exploit Microsoft Graph API

Cybercriminals are exploiting Microsoft's Graph API to facilitate covert communication and control. In a recent cyberattack in Ukraine, a malware named "BirdyClient" leveraged Microsoft OneDrive for stealthy communication and control, posing significant cybersecurity challenges due to the API's integration with commonly used cloud platforms. This reflects an ongoing trend of attackers leveraging the Graph API, as evidenced by past incidents involving various global espionage groups.

Graph's capability to access data and services on Microsoft cloud platforms like Microsoft 365 makes it an ideal choice for command-and-control operations. Attackers are choosing Graph for its stealth and affordability, leveraging free services like OneDrive for secure infrastructure. As awareness of this tactic grows, more attackers are expected to use Graph, necessitating enhanced cybersecurity.

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

Source- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/graph-api-threats

Iranian cyber espionage group APT42 targets global entities

Iranian state-sponsored cyber espionage group APT42, linked to the Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO), employs sophisticated social engineering tactics to target global entities, including NGOs and media outlets. Posing as journalists and event organisers, APT42 gains victims' trust by delivering invitations or authentic documents, allowing them to harvest credentials for accessing cloud environments. Recent operations include deploying custom backdoors like NICECURL and TAMECAT via spear phishing.

APT42's missions align with IRGC-IO's objectives, focusing on monitoring and suppressing perceived threats. Their activities overlap with other reported actors like CALANQUE and Charming Kitten, known for extensive credential harvesting and tailored spear-phishing campaigns. Analysts have identified three infrastructure clusters used by APT42 targeting policy, government, media, and NGO sectors, employing similar tactics across varied domains. Robust security measures are crucial to counter the threat of APT42.

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

Source- https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations

Five Families hacking group claims breach of UAE government servers

On May 2, 2024, the Five Families hacking group claimed to have breached multiple United Arab Emirates government servers, accessing sensitive data. The group demanded a ransom of 150 bitcoins, threatening further data leaks if unpaid by May 9, 2024. The authenticity of these claims remains unverified, sparking concerns about national cybersecurity measures in the UAE.

While the UAE government has not issued an official statement, cybersecurity experts urge a prompt and transparent investigation to assess the extent of the breach. This incident highlights the ongoing challenges faced by governments in safeguarding sensitive data against sophisticated cyber threats. It prompts a re-evaluation of cybersecurity protocols not only in the UAE but potentially globally.

ATTACK TYPE	Ransomware, Breaches	**SECTOR**	Government
REGION	United Arab Emirates	**APPLICATION**	Generic

Source- https://gbhackers.com/hackers-claiming-breach-2/

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