TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: August 13, 2024

THREAT INTELLIGENCE ADVISORY REPORT

Cyber threats pose a growing challenge to organisations worldwide. As the digital landscape evolves, safeguarding data and critical infrastructure is paramount. Businesses must build resilience against a constantly expanding range of cyberattacks. These threats can range from targeted attacks aimed at stealing intellectual property to disruptive ransomware campaigns that cripple operations.

Tata Communications’ weekly threat intelligence advisory offers valuable insights into the latest cyber risks. Organisations can proactively strengthen their defences and mitigate potential vulnerabilities by understanding these threats.

Killer malware disables security software

Killer Ultra, a malware tool used in Qilin ransomware attacks, is threatening Windows systems globally. It can disable popular endpoint detection and response (EDR) and antivirus (AV) tools. The malware exploits a vulnerability (CVE-2024-1853) in the Zemana AntiLogger driver. It also erases Windows Event Logs, hindering forensic analysis. The malware harbours inactive code hinting at potential future functionalities, including downloading malicious tools and bypassing sandbox environments. This dual threat capability underlines the critical need for advanced detection and response strategies.

Due to its application on Windows platforms, strong and adaptive cybersecurity measures are paramount. The emergence of Killer Ultra highlights the ever-evolving nature of cyber threats and the continuous need for enhanced security protocols to protect sensitive data and systems.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.binarydefense.com/resources/blog/technical-analysis-killer-ultra-malware-targeting-edr-products-in-ransomware-attacks/

Microsoft warns of critical flaw in VMware ESXi Software

Microsoft has issued a critical warning regarding a vulnerability (CVE-2024-37085) in VMware ESXi software. This flaw allows cybercriminals to bypass authentication and gain full control of ESXi hypervisors. These hypervisors manage virtual machines, which often house critical business systems. Exploiting this vulnerability, attackers can steal sensitive data, move freely across networks, and encrypt the entire hypervisor's file system, potentially crippling operations. Various threat actors, including Black Basta and Akira, have already exploited this flaw to carry out ransomware attacks.

Organisations are urged to upgrade to the patched version ESXi 8.0 U3 immediately and review their security measures to protect against this threat. This incident highlights the ongoing threat of ransomware and the importance of staying vigilant against emerging vulnerabilities.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	VMWare ESXi

Source - https://thehackernews.com/2024/07/vmware-esxi-flaw-exploited-by.html

INTRODUCTION | KILLER ULTRA DISABLES SECURITY SOFTWARE | MICROSOFT PATCHES VMWARE ESXI | SIDEWINDER TARGETS SHIPPING OPERATIONS | PHISHING SCAM ATTACKS ONEDRIVE USERS | MANDRAKE HIDES IN GOOGLE PLAY APPS | GOOGLE PATCHES CHROME VULNERABILITY | FAKE GOOGLE AUTHENTICATOR ADS DELIVER DEERSTEALER | XDSPY LAUNCHES CYBERESPIONAGE ATTACK | MALWARE TARGETS DEVELOPERS ON ALL PLATFORMS | MINT STEALER STEALS DATA

SideWinder cyberattacks target shipping operations

A state-backed hacking group, SideWinder, believed to be linked to India, is launching cyberattacks against maritime facilities in the Indian Ocean and Mediterranean Sea. The attacks exploit the CVE-2017-0199 vulnerability in Microsoft Office software to spread spear-phishing emails with malicious attachments. These emails target personnel working in ports and maritime facilities in countries like Pakistan, Egypt, and Sri Lanka. The ultimate goal of the attack is suspected to be intelligence gathering on these critical infrastructure points.

SideWinder's campaign has raised significant concerns within the global maritime sector due to its potential to disrupt vital operations and compromise sensitive information. Organisations in the maritime sector are urged to be vigilant against suspicious emails and update their systems with the latest security patches to mitigate the risk.

ATTACK TYPE	Malware	SECTOR	All
REGION	Egypt, Maldives, Myanmar (Burma), Nepal, Pakistan, Sri Lanka	APPLICATION	Windows

Source - https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea

Phishing scam targets OneDrive users

Experts have issued a warning about a phishing scam that targets Microsoft OneDrive users. The scam involves an email containing an HTML file disguised as a OneDrive error notification. Clicking on the file triggers a fake error message prompting users to "fix" the issue by running a command through PowerShell. This command installs malware on the victim's computer. This attack is part of a broader trend of phishing techniques designed to exploit trust in widely used Dapplications.

Named "OneDrive Pastejacking," this campaign has been spotted across several countries. The campaign highlights the urgent need for heightened awareness and robust security measures to protect against such threats. Users are advised to be cautious of unsolicited emails, verify the legitimacy of links, and keep their security software up to date.

ATTACK TYPE	Malware	SECTOR	All
REGION	India, UK, Germany, Ireland, Italy, South Korea, Norway, United States	APPLICATION	Microsoft OneDrive

Source - https://www.trellix.com/blogs/research/onedrive-pastejacking/

INTRODUCTION | KILLER ULTRA DISABLES SECURITY SOFTWARE | MICROSOFT PATCHES VMWARE ESXI | SIDEWINDER TARGETS SHIPPING OPERATIONS | PHISHING SCAM ATTACKS ONEDRIVE USERS | MANDRAKE HIDES IN GOOGLE PLAY APPS | GOOGLE PATCHES CHROME VULNERABILITY | FAKE GOOGLE AUTHENTICATOR ADS DELIVER DEERSTEALER | XDSPY LAUNCHES CYBERESPIONAGE ATTACK | MALWARE TARGETS DEVELOPERS ON ALL PLATFORMS | MINT STEALER STEALS DATA

Mandrake spyware spreads via Google Play apps

Experts have identified a new variant of the Android spyware "Mandrake" in five Google Play apps, which were collectively downloaded 32,000 times. Mandrake has been lurking undetected since at least 2016, and the new version features better obfuscation and evasion tactics. Once the malware is activated, it can perform a wide range of malicious activities such as data collection, screen recording and monitoring, command execution, simulation of user swipes and taps, file management, and app installation.

Users are strongly advised to be cautious when installing apps and to ensure Google Play Protect is active to mitigate potential risks. The persistence of Mandrake underscores the importance of maintaining vigilant cybersecurity practices, including regular updates and scrutinising app permissions.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Android

Source - https://www.bleepingcomputer.com/news/security/android-spyware-mandrake-hidden-in-apps-on-google-play-since-2022/

Google urgently fixes critical Chrome vulnerability

Google has issued an urgent security update to fix a critical vulnerability CVE-2024-6990, found in the Dawn component of Chrome. This vulnerability could open the door for malicious code execution. Security researcher “gelatin dessert” discovered this flaw on July 15th. Attackers could have potentially exploited this vulnerability to install malware, steal sensitive data, or perform other harmful actions. The update also addressed two other high-risk vulnerabilities (CVE-2024-7255 and CVE-2024-7256). These vulnerabilities affect all sectors globally, emphasising the need for immediate action.

Users are strongly urged to update their Chrome browsers immediately to ensure their security and protect against potential exploits. The rapid response from Google underscores the seriousness of these threats and the importance of maintaining up-to-date software.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	Chrome

Source - https://securityonline.info/urgent-chrome-update-google-patches-critical-security-flaw-cve-2024-6990/

Malware delivered via Fake Google Authenticator ads

Hackers are using fake Google ads to spread malware disguised as the genuine Google Authenticator app. Clicking these ads takes users to a bogus download page that mimics the official download page, tricking them into downloading DeerStealer malware. DeerStealer malware is designed to steal sensitive personal data such as banking credentials, passwords, and credit card details. This threat affects all sectors globally and targets users of Google Chrome OS.

To safeguard against such threats, users are advised to avoid clicking on ads for downloads, verify websites and URLs carefully, use updated antivirus software, and enable multi-factor authentication. This discovery highlights the persistent risk of malware distribution through seemingly legitimate channels and underscores the importance of cautious online behaviour.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Google Chrome OS

Source - https://www.malwarebytes.com/blog/news/2024/07/threat-actor-impersonates-google-via-fake-ad-for-authenticator

XDSpy launches cyberespionage attack

A cyberespionage group known as XDSpy has launched a phishing campaign targeting companies in Russia and Moldova. The attack uses malicious emails to deploy malware called DSDownloader, capable of stealing sensitive information. XDSpy, active since 2011, uses clever tactics like spear-phishing emails that appear legitimate. These emails trick recipients into clicking malicious links or downloading infected attachments, ultimately installing the data-stealing malware.

As tensions rise due to the Russia-Ukraine conflict, cyberattacks are on the increase as various threat actors exploit geopolitical tensions to conduct espionage activities. Businesses are urged to be vigilant against such threats and enhance their cybersecurity measures, including strong email filtering, employee training on phishing awareness, and up-to-date security software.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	All
REGION	Russia, Moldova	APPLICATION	Windows

Source - https://thehackernews.com/2024/07/cyber-espionage-group-xdspy-targets.html

Malware targets developers on all platforms

A North Korean-linked malware campaign, DEV#POPPER, is targeting developers across Windows, Mac, and Linux systems. Hackers use social engineering tactics to trick them into downloading malware disguised as job interview opportunities on GitHub. This attack leads to data exfiltration and system compromise, where developers are lured into compromising their own systems. Once downloaded, the malware can steal data and potentially hijack devices.

The campaign's evolution to include multi-stage payloads and advanced obfuscation techniques highlights the growing sophistication of the threat. To protect against such threats, developers and organisations are urged to verify the legitimacy of software sources, maintain up-to-date security measures, and be cautious of unsolicited job offers or requests.

ATTACK TYPE	Malware	SECTOR	All
REGION	North America, Middle East, Europe, South Korea	APPLICATION	Apple MacOS, Windows, Linux

Source - https://www.securonix.com/blog/research-update-threat-actors-behind-the-devpopper-campaign-have-retooled-and-are-continuing-to-target-software-developers-via-social-engineering/

INTRODUCTION | KILLER ULTRA DISABLES SECURITY SOFTWARE | MICROSOFT PATCHES VMWARE ESXI | SIDEWINDER TARGETS SHIPPING OPERATIONS | PHISHING SCAM ATTACKS ONEDRIVE USERS | MANDRAKE HIDES IN GOOGLE PLAY APPS | GOOGLE PATCHES CHROME VULNERABILITY | FAKE GOOGLE AUTHENTICATOR ADS DELIVER DEERSTEALER | XDSPY LAUNCHES CYBERESPIONAGE ATTACK | MALWARE TARGETS DEVELOPERS ON ALL PLATFORMS | MINT STEALER STEALS DATA

Mint Stealer malware steals sensitive data

Experts have issued an urgent warning against Mint Stealer, a sophisticated Python-based malware functioning as a malware-as-a-service (MaaS) tool. It is designed to extract sensitive data from various sources such as web browsers, cryptocurrency wallets, and gaming accounts. This malware uses advanced encryption and obfuscation techniques to evade detection, thus making it a challenging threat to quickly identify and mitigate. Mint Stealer is marketed through specialised websites and supported via Telegram, highlighting its commercial nature and the increasing sophistication of cyber threats. The malware’s ability to target a broad range of applications and sectors underscores its potential impact. Mint Stealer targets all sectors globally. It specifically attacks Windows systems.

Organisations globally must implement tight cybersecurity measures to defend against such evolving threats. This includes employing advanced security solutions, regularly updating systems, and educating users about the risks of malware.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.cyfirma.com/research/mint-stealer-a-comprehensive-study-of-a-python-based-information-stealer/

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.