TATA COMMUNICATIONS

TATA

# YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: DECEMBER 3, 2024

# THREAT INTELLIGENCE ADVISORY REPORT

In today’s landscape of complex and evolving cybersecurity threats, individuals, businesses, and government entities face growing challenges in maintaining operational security. Protecting against disruptions, financial losses, and reputational damage requires robust digital defences to ensure the integrity, confidentiality, and availability of critical data.

Our weekly Cyber Threat Intelligence (CTI) report keeps you informed about emerging global threats, providing actionable insights to strengthen your security measures. Paired with our expert advisory services, we help safeguard your IT assets against persistent risks. Leverage our intelligence to enhance your organisation’s security posture and build a resilient, secure future.

# SafePay ransomware emerges with exfiltration and encryption tactics

Analysts have discovered SafePay, a sophisticated ransomware strain linked to advanced techniques and older ransomware families like LockBit. Known for its stealth, SafePay appends a .safepay extension to encrypted files and issues ransom notes titled readme_safepay.txt. Researchers believe its creators may have utilised leaked LockBit source code, enhancing its capabilities.

SafePay operates through a two-phase attack model: data exfiltration and encryption. Attackers archive files using WinRAR and exfiltrate them via FileZilla, removing traces post-operation. After that, using RDP and PowerShell scripts, they encrypt network shares, disable recovery systems, and demand negotiations via ominous ransom notes. Advanced features include UAC bypass, anti-analysis techniques, and a Cyrillic language-based kill switch to avoid Eastern European targets. With a presence on TOR and TON networks, SafePay's leak site exposes stolen data and operational vulnerabilities, offering rare insights into this emerging cyber threat.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://securityonline.info/safepay-ransomware-a-new-threat-with-sophisticated-techniques/

# New threat actors Earth Estries poised to wreak havoc globally

Earth Estries, an advanced threat group, employs two distinct attack chains targeting governments and the tech industry. Both chains exploit vulnerabilities in systems like Microsoft Exchange servers and adapter management tools, showcasing technical sophistication and adaptability. The first chain uses CAB-delivered tools like Cobalt Strike, Hemigate, and Crowdoor for lateral movement via PsExec, with Trillclient harvesting credentials from browser caches. The second chain leverages malware like Zingdoor and SnappyBee, delivered through cURL, alongside web shells and DLL sideloading to maintain persistence and escalate privileges.

Earth Estries combines advanced tools, strategic exploitation, and a deep understanding of target environments to maintain prolonged access. Defenders should focus on securing external-facing systems, patching vulnerabilities, and implementing robust credential management to mitigate such sophisticated threats.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html

# Iranian state-backed malware indulges in cyberespionage

Cybersecurity researchers have uncovered WezRat, a remote access trojan (RAT) and information stealer linked to Iranian state-sponsored actors, Cotton Sandstorm. First detected in September 2023, WezRat is used for reconnaissance, data theft, and executing malicious commands on compromised systems. WezRat can execute commands, take screenshots, steal clipboard content and cookies, and perform keylogging. Its modular design allows additional capabilities to be downloaded as DLL files, minimising suspicion of the main backdoor component.

The malware spreads through phishing emails impersonating the Israeli National Cyber Directorate (INCD). Victims are tricked into installing a trojanised Google Chrome installer that launches a malicious binary (Updater.exe), which connects to a command-and-control (C2) server for further instructions. Analysis suggests two development teams are refining WezRat, signalling a significant investment in its evolution as a versatile cyberespionage tool.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Israel, US, Middle East | APPLICATION | Windows |

Source - https://thehackernews.com/2024/11/iranian-hackers-deploy-wezrat-malware.html

# Water Barghest botnet exploiting IoT for proxy monetisation

Researchers have uncovered Water Barghest, a sophisticated botnet that has compromised over 20,000 IoT devices by October 2024 to establish a highly automated residential proxy network. By exploiting vulnerabilities, including a 2023 Cisco IOS XE zero-day flaw, the group rapidly converts devices into proxies for cybercriminal activities. Leveraging internet scanning tools like Shodan, Water Barghest deploys Ngioweb, a stealthy memory-resident malware, registering infected devices with C2 servers. Within 10 minutes, compromised IPs appear on residential proxy marketplaces, used for data scraping, bypassing restrictions, or launching anonymised cyberattacks.

The botnet's automation and swift monetisation highlight the risks posed by insecure IoT devices. Researchers warn enterprises and individuals to minimise IoT exposure to the open internet, apply strong access controls, and maintain regular firmware updates to mitigate threats from botnets like Water Barghest. This discovery emphasises the evolving sophistication of proxy botnets in cybercrime.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Global | APPLICATION | Windows, Linux |

Source - https://securityonline.info/water-barghest-botnet-hijacks-20000-iot-devices-for-profit/

# Helldown ransomware expands to target virtualised environments

Cybersecurity researchers have identified a Linux variant of Helldown ransomware, signalling an expansion of attack vectors by threat actors. Initially derived from the LockBit 3.0 code, Helldown is now targeting virtualised infrastructures like VMware, with recent focus on ESX environments. First documented in August 2024, Helldown is an aggressive ransomware group that exploits vulnerabilities in sectors such as IT, telecommunications, manufacturing, and healthcare.

Known for using double extortion tactics, the group has attacked at least 31 organisations within three months. Additionally, Zyxel issued an advisory after discovering its firewalls were targeted by the group, urging customers to update firmware and change passwords to mitigate these threats.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Ransomware | SECTOR | Healthcare, manufacturing, IT, telecommunications |
| REGION | Global | APPLICATION | VMware ESX, Linux |

Source - https://thehackernews.com/2024/11/new-helldown-ransomware-expands-attacks.html

INTRODUCTION | SAFEPAY RANSOMWARE DISRUPTS OPERATIONS | EARTH ESTRIES TARGETS GOVERNMENT AND TECH ENTITIES | WEZRAT SPIES ON WESTERN ORGANISATIONS | WATER BARGHEST BOTNET COMPROMISES IOT DEVICES | HELLDOWN TARGETS VIRTUALISED ENVIRONMENTS | JOBSEEKERS BEING LURED BY DPRK CYBER GROUP | BABBLELOADER EVADES AI DETECTION SYSTEMS | APPLE VULNERABILITIES EXPLOITED BY THREAT ACTORS | FROSTYGOOP ATTACKS UKRAINIAN INFRASTRUCTURE | EARTH KASHA SETS SIGHT ON NEW TARGETS

# North Korean cyber group targets jobseekers with phishing and malware

A recent report reveals a sophisticated phishing campaign by North Korean cyber group CL-STA-0237, linked to illicit state activities, including weapons development. Initially targeting JavaScript developers via npm packages, the group now uses fake video conferencing apps like MiroTalk and FreeConference to spread malware. Victims, lured by fraudulent job offers, download malware-laden installers, leading to the BeaverTail malware and InvisibleFerret RAT, providing attackers with remote access to steal data and further compromise systems.

CL-STA-0237 employs fake resumes, often with altered headshots, to infiltrate companies and secure remote positions. These tactics are tied to broader North Korean cyber operations like the Wagemole Campaign, which funds weapons programs through cyberespionage and financial theft. Researchers recommend strengthening hiring practices, monitoring for insider threats, and scrutinising third-party services to defend against such evolving threats.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | IT |
| REGION | Global | APPLICATION | Windows |

Source - https://securityonline.info/north-korean-hackers-target-job-seekers-with-malware-laced-video-apps/

# BabbleLoader evades detection by outsmarting AI systems

BabbleLoader, a highly sophisticated malware loader, is employing advanced evasion techniques to bypass both traditional and AI-based detection systems. Key tactics include junk code insertion, metamorphic transformations, dynamic API resolution, and shellcode loading, all of which obfuscate its true function and evade signature-based and behavioural detections. These methods disrupt AI's ability to analyse and detect malware by overwhelming pattern recognition systems with irrelevant data, such as junk variables and instructions that mislead AI models into false predictions.

This loader has been observed in various campaigns, targeting a wide range of users – from individuals seeking cracked software to business professionals in finance and administration. The constant variation in its code forces AI systems to continuously relearn detection methods, making it increasingly difficult to detect. BabbleLoader also incorporates anti-sandboxing features and demonstrates the developer's commitment to adapting to the latest security research, ensuring that it remains resilient to evolving defences.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://intezer.com/blog/research/babble-babble-babble-babble-babble-babble-babbleloader/

# Zero-day vulnerabilities exposed in various Apple products

Apple has urged users to update their devices after two critical zero-day vulnerabilities – CVE-2024-44308 and CVE-2024-44309 – were discovered and actively exploited. These flaws, affecting iPhones, iPads, Macs, and the Vision Pro headset, were found in Apple's JavaScriptCore and WebKit frameworks. The vulnerabilities pose serious risks, including arbitrary code execution and cross-site scripting (XSS) attacks, potentially compromising user data and security.

CVE-2024-44308 could allow attackers to execute arbitrary code by exploiting maliciously crafted web content, while CVE-2024-44309 enables XSS, potentially exposing user cookies and session data. Apple has addressed both issues with enhanced security checks and improved cookie management. These flaws primarily impact devices running iOS 17.7.2, iPadOS 17.7.2, macOS Sequoia 15.1.1, and visionOS 2.1.1. Users are strongly advised to install the latest updates immediately to protect against these active threats.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Vulnerability | SECTOR | All |
| REGION | macOS, iOS | APPLICATION | Global |

Source - https://securityonline.info/cve-2024-44308-and-cve-2024-44309-apple-addresses-zero-day-vulnerabilities/

# FrostyGoop malware grows as a threat to critical infrastructure

An OT-focused malware, FrostyGoop (aka BUSTLEBERM) came to light recently after it disrupted heating services for over 600 Ukrainian apartment buildings during sub-zero temperatures. The Cyber Security Situation Centre (CSSC) attributed the attack to Russian actors, targeting a municipal energy company through vulnerabilities in its ICS/OT systems. FrostyGoop is the ninth known ICS-centric malware and the first to exploit the widely used Modbus TCP protocol, enabling direct manipulation of industrial control systems.

The malware can operate internally within a compromised network or externally on exposed devices. It sends malicious Modbus commands to alter system measurements, disrupt operations, and damage infrastructure. Analysis revealed configuration files and libraries linked to the malware, along with telemetry indicating over 1 million Modbus TCP devices exposed online globally between September and October 2024. The attack underscores the growing risk of OT cyberattacks, driven by the increasing integration of IT and OT networks.

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

Source - https://unit42.paloaltonetworks.com/frostygoop-malware-analysis/

INTRODUCTION | SAFEPAY RANSOMWARE DISRUPTS OPERATIONS | EARTH ESTRIES TARGETS GOVERNMENT AND TECH ENTITIES | WEZRAT SPIES ON WESTERN ORGANISATIONS | WATER BARGHEST BOTNET COMPROMISES IOT DEVICES | HELLDOWN TARGETS VIRTUALISED ENVIRONMENTS | JOBSEEKERS BEING LURED BY DPRK CYBER GROUP | BABBLELOADER EVADES AI DETECTION SYSTEMS | APPLE VULNERABILITIES EXPLOITED BY THREAT ACTORS | FROSTYGOOP ATTACKS UKRAINIAN INFRASTRUCTURE | EARTH KASHA SETS SIGHT ON NEW TARGETS

# Earth Kasha expands cyber operations with new tools and targets

LODEINFO, a malware active since 2019, is a hallmark of Earth Kasha, a group targeting Japan. While some link Earth Kasha to APT10, evidence remains insufficient, prompting the term “APT10 Umbrella” to describe overlapping operations and tools. Earth Kasha has now launched a new campaign, expanding targets to high-profile organisations in Japan, Taiwan, and India, focusing on advanced technology and government sectors. This campaign marked a shift in tactics, exploiting public-facing applications like SSL-VPNs and file storage services through vulnerabilities in products such as Array AG (CVE-2023-28461) and FortiOS (CVE-2023-27997).

Earth Kasha deployed backdoors like Cobalt Strike, LODEINFO, and the novel NOOPDOOR, often delivered using GOSICLOADER, a shellcode loader leveraging DLL side-loading. Connections to Earth Tengshe and other China-aligned groups suggest shared tools and tactics among threat actors, underscoring the growing complexity of attribution in cyberespionage campaigns targeting critical infrastructure.

| | | | |
|---|---|---|---|
| ATTACK TYPE | Malware | SECTOR | All |
| REGION | Global | APPLICATION | Windows |

Source - https://www.trendmicro.com/en_us/research/24/k/lodeinfo-campaign-of-earth-kasha.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*

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.