
YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: October 29, 2024



THREAT INTELLIGENCE ADVISORY REPORT

Today's fast-evolving digital landscape is creating increasingly complex cybersecurity threats for individuals, businesses, and governments leading to operational disruptions, financial losses, and reputational damage. In such a scenario, safeguarding the integrity, confidentiality, and availability of your enterprise data hinges on strengthening your digital defences.

Our weekly reports offer up-to-date cyber threat intelligence helping you stay ahead of emerging threats. Moreover, our comprehensive advisory services safeguard your IT assets from persistent risks. In an age where cyber resilience is crucial, leverage our threat intelligence reports for critical insights and enhance the security posture of your organisation.

INTRODUCTION

LOW-COST, HIGH-RISK, DARKVISION THREAT

IVANTI CSA EXPLOITS ZERO-DAY VULNERABILITY

EDRSILENCER BYPASSES MALWARE DETECTION

LINUX FASTCASH MALWARE MANIPULATES ATMS

SOLARWINDS VULNERABILITY ALTERS SENSITIVE DATA

MALWARE EXPLOITS CODE-SIGNING CERTIFICATE

WORDPRESS VULNERABILITY THREATENS WEBSITES

STATE-SPONSORED CYBERATTACKS ON INDIAN MSMES

NORTH-KOREAN ACTORS EXPLOIT WINDOWS VULNERABILITY

SIDEWINDER APT TOOL COMPROMISES SYSTEMS

The low-cost, high-risk threat of the DarkVision RAT

Researchers have conducted in-depth analysis of the DarkVision RAT, a highly customisable and affordable remote access trojan (RAT). The analysis highlights the RAT’s evolution and increased sophistication since its emergence in 2020. Priced at just \$60, this malware has gained popularity among cybercriminals due to its affordability and extensive feature set, which includes keylogging, file manipulation, password theft, and remote code execution.

The analysis further reveals DarkVision RAT’s use of advanced evasion techniques like DLL hijacking and auto-elevation to bypass security defences. Recent campaigns revealed its distribution with PureCrypter malware, employing multiple persistence methods and encrypted plugins to maintain access. With its adaptability and low cost, DarkVision RAT is expected to remain a key tool for attackers, providing significant capabilities for data theft and system compromise.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - <https://securityonline.info/darkvision-rat-the-60-malware-threatening-your-data/>

Zero-day vulnerabilities exploited in Ivanti CSA for persistent access & control

Fortinet FortiGuard Labs reports the exploitation of three zero-day vulnerabilities in Ivanti Cloud Service Appliance (CSA) by a suspected nation-state adversary to carry out malicious actions. These vulnerabilities include CVE-2024-8190 (command injection), CVE-2024-8963 (path traversal), and CVE-2024-9380 (authenticated command injection) and enabled unauthorised access, enumeration of users, and the theft of credentials. The attackers used the stolen admin credentials to drop a web shell maintaining persistent access and later patched the vulnerabilities to block other intruders.

The adversaries also exploited a critical flaw, CVE-2024-29824, in Ivanti Endpoint Manager (EPM) that unlocked remote code execution (RCE). This involved creating new users, performing reconnaissance, exfiltrating data using DNS tunnelling, and deploying a rootkit to ensure persistence. The severity of the threat was further underscored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) which added these vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue in October 2024.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Generic, Ivanti

Source - <https://thehackernews.com/2024/10/nation-state-attackers-exploiting.html>

EDRSilencer tool bypasses endpoint detection and conceals malware

The use of the open-source EDRSilencer tool to tamper with endpoint detection and response (EDR) solutions and conceal malicious activity is on the rise. The tool works by identifying running EDR processes and configuring WFP filters. It was originally designed for red teaming. However, EDRSilencer is now used to hamper network communications allowing malicious activity to evade detection by blocking security software from sending telemetry to management consoles. Security software often fail to detect and contain the malware as it targets multiple EDR products, including those from Microsoft, SentinelOne, and Palo Alto Networks.

The use of tools like EDRSilencer highlights a broader trend of attackers incorporating EDR-killing utilities like AuKill and EDRKillShifter, to enhance persistence and disable security processes. This underscores the spiralling sophistication of ransomware groups in terms of their ability to bypass traditional defence mechanisms.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - <https://thehackernews.com/2024/10/hackers-abuse-edrsilencer-tool-to.html>

Threat actors use the Linux variant of FASTCash malware for ATM cashout schemes

A Linux variant of the FASTCash malware is being deployed by North Korean threat actors to steal funds through ATM cashout schemes, reports security researcher HaxRob. The malware is installed on compromised payment switch servers intercepting and manipulating ISO 8583 transaction messages to allow unauthorised withdrawals from ATMs. The new Linux variant was first detected in mid-2023 targeting Ubuntu Linux 20.04 and manipulating transaction messages to approve unauthorised withdrawals in Turkey, ranging between ₺12,000 and ₺30,000 (\$350 and \$875). This highlights the escalating threat to Linux server environments, which often lack sufficient detection capabilities.

However, the malware was first documented in 2018 and has been leveraged by North Korean-linked groups such as HIDDEN COBRA in bank attacks across Africa and Asia. These schemes have facilitated Simultaneous ATM withdrawals across multiple countries have been facilitated by these schemes so far with one incident enabling cashouts in 30 countries.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Linux

Source - <https://thehackernews.com/2024/10/new-linux-variant-of-fastcash-malware.html>

INTRODUCTION	LOW-COST, HIGH-RISK, DARKVISION THREAT	IVANTI CSA EXPLOITS ZERO-DAY VULNERABILITY	EDRSILENCER BYPASSES MALWARE DETECTION	LINUX FASTCASH MALWARE MANIPULATES ATMS	SOLARWINDS VULNERABILITY ALTERS SENSITIVE DATA	MALWARE EXPLOITS CODE-SIGNING CERTIFICATE	WORDPRESS VULNERABILITY THREATENS WEBSITES	STATE-SPONSORED CYBERATTACKS ON INDIAN MSMES	NORTH-KOREAN ACTORS EXPLOIT WINDOWS VULNERABILITY	SIDEWINDER APT TOOL COMPROMISES SYSTEMS
--------------	--	--	--	--	--	---	--	--	---	---

Critical SolarWinds vulnerability added to CISA’s KEV catalogue

A critical vulnerability in SolarWinds Web Help Desk (WHD) software has been added by the CISA, tracked as CVE-2024-28987 (CVSS score: 9.1), to its KEV catalogue. The flaw involves hard-coded credentials that allow remote, unauthenticated attackers to access internal functionality and alter sensitive data.

This was first disclosed in August 2024 with technical specifics released by Horizon3.ai in September. The vulnerability enables attackers to read and alter helpdesk tickets with confidential information like passwords and shared service account credentials. Even as the details of active exploitation are unclear, this marks the second WHD vulnerability added to the KEV catalogue in recent months. As a response, Federal Civilian Executive Branch (FCEB) agencies are recommended to apply the latest fixes by November 5, 2024, to secure their networks.

ATTACK TYPE	Vulnerability	SECTOR	All
REGION	Global	APPLICATION	SolarWinds

Source - <https://thehackernews.com/2024/10/cisa-warns-of-active-exploitation-in.html>

Malware campaign exploits legitimate code-signing certificates

Researchers have uncovered a new malware campaign using Hijack Loader, also known as DOILoader, signed with legitimate code-signing certificates. The campaign was first detected in early October 2024 by French cybersecurity firm HarfangLab. Attackers have deployed Lumma, an information stealer, through social engineering which tricks victims by running malicious PowerShell commands disguised as CAPTCHA verifications.

Hijack Loader’s attack chain involves downloading a ZIP file containing a legitimate executable vulnerable to DLL side-loading, alongside a malicious DLL. This enables the malware to remain undetected. Recent updates show attackers using signed binaries to further evade security measures, with the certificates potentially being stolen or fraudulently obtained. With more and more malicious actors exploiting this method, the dangers of relying solely on code-signing for trust come to the forefront. Additional malware like XWorm and CoreWarrior has also been observed, showcasing the evolving tactics used to compromise Windows systems.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - <https://thehackernews.com/2024/10/researchers-uncover-hijack-loader.html>

WordPress plugin vulnerabilities exposed

A critical security vulnerability (CVE-2024-9634) has been identified and fixed in GiveWP, a widely used WordPress donation plugin with over 100,000 active installations. This PHP Object Injection flaw could allow unauthenticated attackers to execute arbitrary code on affected websites, potentially compromising sensitive donor information and gaining full control of the site.

Additionally, earlier today, Jetpack, a popular WordPress plugin by Automattic, released a critical security update to fix a vulnerability that allowed logged-in users to access forms submitted by other site visitors. Jetpack, installed on 27 million websites, offers tools to improve website functionality, security, and performance. The vulnerability, affecting all Jetpack versions since 3.9.9 (released in 2016), was discovered during an internal audit. Even though there is no evidence to link these vulnerabilities with any form of exploitation yet, both developers are urging users to update the respective plugins in a bid to prevent any potential attacks.

ATTACK TYPE	Vulnerability	SECTOR	Aviation, BFSI, construction, defence, energy, government, healthcare, IT, manufacturing, mining, oil and gas, pharmaceuticals, telecommunications
REGION	Global	APPLICATION	WordPress

Source - <https://securityonline.info/critical-security-vulnerability-in-jetpack-plugin-affects-millions-of-wordpress-websites/>

Indian MSMEs face rising cyber threats from state-sponsored attackers

India’s growing economic activities, particularly in manufacturing, IT, financial services, e-commerce, and pharmaceuticals, are attracting financially motivated and state-sponsored cyber threat actors from countries like Russia, China, Pakistan, and North Korea. The attacks, including DDoS and website defacement, are disrupting online services and altering websites to spread political messages. The surge in e-commerce and digital payments in the post-pandemic era has intensified these threats. These attacks cause not only financial and reputational damage, but also deter potential global investors.

Moreover, the adoption of emerging technologies, such as internet of things (IoT), cloud computing, and artificial intelligence (AI), presents new cybersecurity challenges. Particularly affected are the micro, small, and medium enterprises (MSMEs), which face significant risks due to financial constraints and exposes the broader supply chain to potential compromises.

ATTACK TYPE	Hacktivist/DDoS	SECTOR	Aviation, BFSI, construction, defence, energy, government, healthcare, IT, manufacturing, mining, oil and gas, pharmaceuticals, telecommunications
REGION	India	APPLICATION	Generic

Source - <https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-asia-pacific-apac-region-volume-1-2/>

ScarCruft exploits Windows zero-day vulnerability using malicious toast ads

North Korean threat actor, ScarCruft, also known as TA-RedAnt or APT37, has been linked to a zero-day exploit targeting a now-patched Windows vulnerability (CVE-2024-38178). This memory corruption bug in the Scripting Engine permits remote code execution, exploited via the Edge browser in Internet Explorer Mode. Microsoft helped patch this vulnerability consisting of a CVSS score of 7.5 in 2024.

Tools used by ScarCruft to exploit the flaw included malicious “toast” advertisements, free software, and injection of exploitation code into compromised ad servers. The malware, RokRAT, delivered through these attacks, acts by enabling file enumeration, process termination, command execution, and data extraction from applications like browsers and messaging platforms. Cloud services like Dropbox and Google Cloud are leveraged as well for command-and-control operations, rendering the job undetectable. This is how ScarCruft exploits vulnerabilities in legacy systems, emphasising the need for regular security updates to mitigate future risks.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - <https://thehackernews.com/2024/10/north-korean-scarcruft-exploits-windows.html>

SideWinder expands global operations and deploys advanced malware

The SideWinder Advanced Persistent Threat (APT) group, also known as T-APT-04 or RattleSnake has predominantly targeted South and Southeast Asia since its appearance in 2012. SideWinder has emerged as a formidable force in global cyber espionage and has recently expanded its operations to the Middle East, Africa, and strategic sectors such as telecommunications and logistics.

Researchers have informed that SideWinder now deploys a sophisticated post-exploitation tool called “StealerBot,” capable of password theft, keylogging, and remote control of compromised systems. The detection of StealerBot is difficult as it operates entirely in memory. SideWinder’s typical attack chain begins with spear-phishing and the exploitation of CVE-2017-11882, with many campaigns mimicking government entities. Thus, SideWinder’s operations reveal the complexity that challenges defenders worldwide, despite being a low-skilled actor.

ATTACK TYPE	Malware	SECTOR	Education, oil and gas, telecommunications, logistics and shipping
REGION	Middle East, Africa, India, Afghanistan, China, France, Indonesia	APPLICATION	Windows

Source - <https://securityonline.info/sidewinder-apt-a-decade-of-evolution-and-global-expansion/>

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.