Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

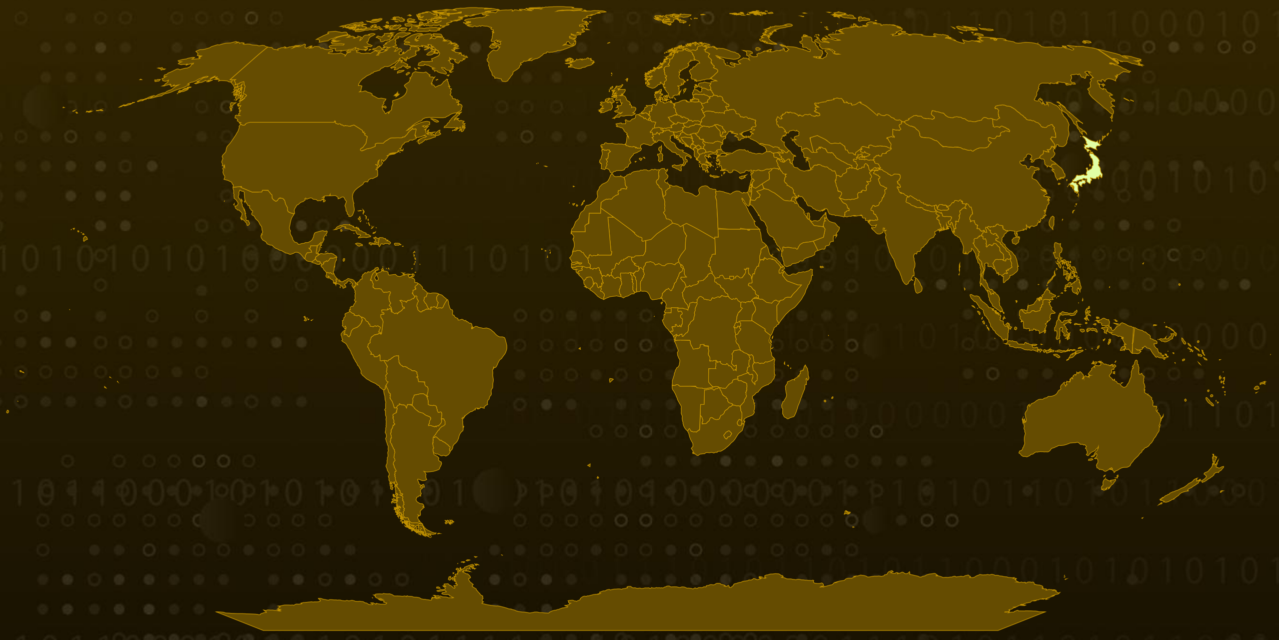
MostereRAT: A Deep Dive into an EPL-Backed Phishing Operation

Date of Publication	Admiralty Code	TA Number
September 10, 2025	A1	TA2025276

Summary

Attack Discovered: 2025
Targeted Countries: Japan
Affected Platform: Windows
Malware: MostereRAT
Attack: Attackers have launched a crafty phishing campaign in Japan that does far more than just trick users into clicking a bad link. Hidden behind what looks like a simple email lure is MostereRAT, a stealthy Remote Access Trojan that quietly slips into systems, disguising itself with celebrity images, creating fake services, and even shutting down security protections to stay invisible. What makes it especially dangerous is its use of Easy Programming Language (EPL) and secure, encrypted channels to stage payloads, block defenses, and give attackers complete remote control. By combining social engineering with highly advanced evasion, this campaign turns a single careless click into a full system compromise.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 A sophisticated phishing campaign has surfaced, targeting Japanese users with highly evasive techniques and a well-orchestrated infection chain. The operation begins with deceptive emails that lure victims into clicking malicious links disguised as legitimate sources. Once the link is accessed, a malicious file is downloaded automatically, followed by a booby-trapped Word document containing an embedded archive. The victim is instructed to extract and run the file, unknowingly setting the stage for infection. At the heart of this campaign lies MostereRAT, a Remote Access Trojan that has steadily evolved into a powerful espionage tool.

#2 The initial executable ("document.exe") is bundled with celebrity images, disguising its malicious payload. A simple decryption technique unlocks the next stage, which is planted in the ProgramData folder and executed with elevated privileges by directly interfacing with the Windows Service Control Manager. Two malicious services are created to run scripts and launch modules, while the program throws a fake message in Simplified Chinese as a smokescreen.

#3 A key innovation in this campaign is the abuse of Easy Programming Language (EPL), a beginner-friendly Chinese scripting environment. Attackers leverage its ability to compile modules into EPK files, which can be decrypted and loaded dynamically in memory. These modules expand the malware's capabilities, ranging from executing scheduled jobs through XML-defined tasks to creating hidden services with SYSTEM or even TrustedInstaller privileges. This grants the attackers deep control over the compromised system, allowing them to re-launch instances, escalate rights, and maintain stealthy persistence.

#4 The evolution of MostereRAT also highlights its advanced defense evasion. It maintains built-in lists of security tools and actively blocks their communication, echoing red-team utilities like EDRSilencer. The malware terminates critical processes, halts update services, deletes system files, and removes scheduled tasks to weaken protections. Communication with command-and-control infrastructure is equally sophisticated, using SHA-256 validation and secure connections over HTTP, TCP, and even mutual TLS authentication (mTLS) to prevent impersonation.

#5 MostereRAT's arsenal extends beyond custom modules, enabling attackers to run third-party tools like AnyDesk, TigerVNC, Xray, and RDP Wrapper for remote control. It logs keystrokes, monitors active windows, captures screens, and exfiltrates files with surgical precision. Persistence is further reinforced by creating hidden accounts with non-expiring credentials that never appear on the login screen. By blending advanced programming techniques, service manipulation, security bypasses, and social engineering, this campaign poses a formidable challenge for defenders.

Recommendations

Be cautious with email links and attachments: If you receive an unexpected email, especially one that urges you to click a link or open a file, take a moment to verify the sender. Attackers often disguise malicious files as something familiar to trick you into opening them.

Use reliable security tools: Ensure you have up-to-date antivirus and endpoint protection. These tools can detect unusual behavior, like attempts to stop security services or block updates.

Watch for unusual system behavior: Unexpected messages, unknown services running in the background, or new accounts appearing on your system could be signs of infection. Report and investigate these anomalies quickly.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1566** Phishing	**T1566.002** Spearphishing Link	**T1204** User Execution
T1204.001 Malicious Link	**T1204.002** Malicious File	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1547 Boot or Logon Autostart Execution	**T1070** Indicator Removal	**T1053** Scheduled Task/Job	**T1574** Hijack Execution Flow

T1574.001 DLL	**T1113** Screen Capture	**T1059** Command and Scripting Interpreter	**T1090** Proxy
T1136 Create Account	**T1056** Input Capture	**T1021** Remote Services	**T1033** System Owner/User Discovery
T1036 Masquerading	**T1203** Exploitation for Client Execution	**T1543** Create or Modify System Process	**T1068** Exploitation for Privilege Escalation
T1562 Impair Defenses	**T1082** System Information Discovery	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	www[.]efu66[.]com, mostere[.]com, huanyu3333[.]com, idkua93dkh9590764478t18822056bck[.]com, osjfd923bk78735547771x3690026ddl[.]com, zzzzzzz0379098305467195353458278[.]com, xxxxxx2543369372808014085091644 4[.]com
SHA256	d281e41521ea88f923cf11389943a046557a2d73c20d30b64e02af1c04c64ed1, 4e3cdeba19e5749aa88329bc3ac67acd777ea7925ba0825a421cada083706a4e, 546a3418a26f2a83a2619d6c808985c149a0a1e22656553ce8172ca15622fd9b, 3c621b0c91b758767f883cbd041c8ef701b9806a78f2ae1e08f932b43fb433bb, 926b2b9349dbd4704e117304c2f0edfd266e4c91fb9325ecb11ba83fe17bc383

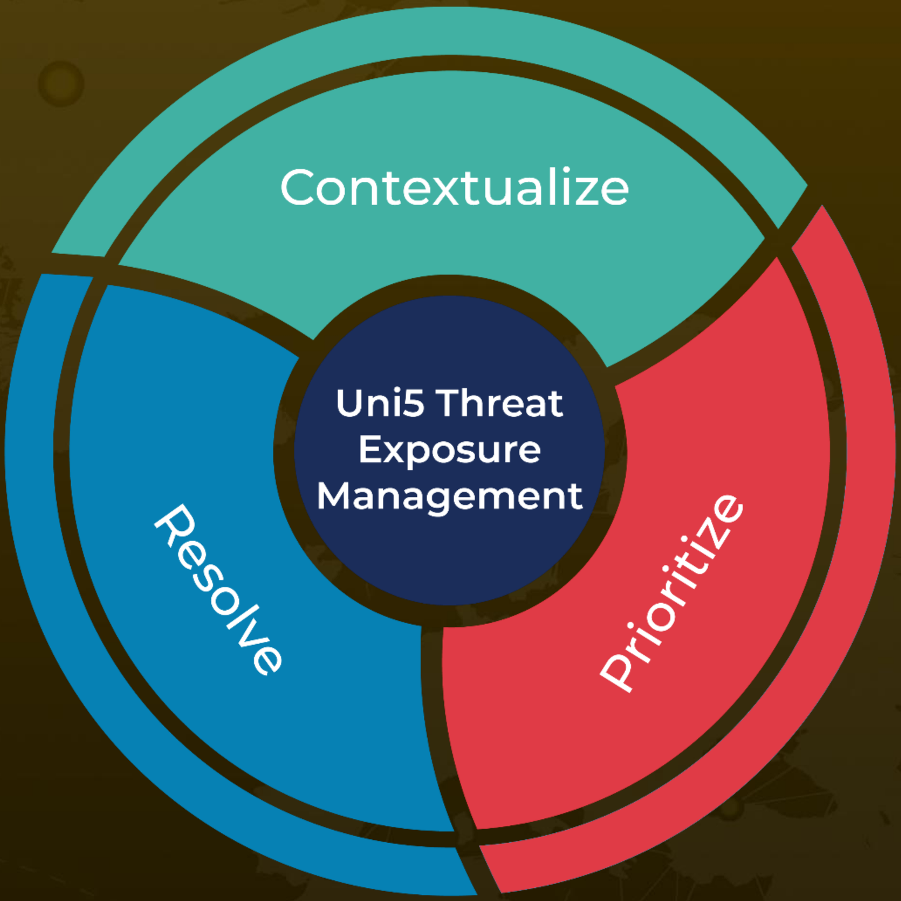
References

https://www.fortinet.com/blog/threat-research/mostererat-deployed-anydesk-tightvnc-for-covert-full-access

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 10, 2025 • 5:15 AM

More at www.hivepro.com