Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

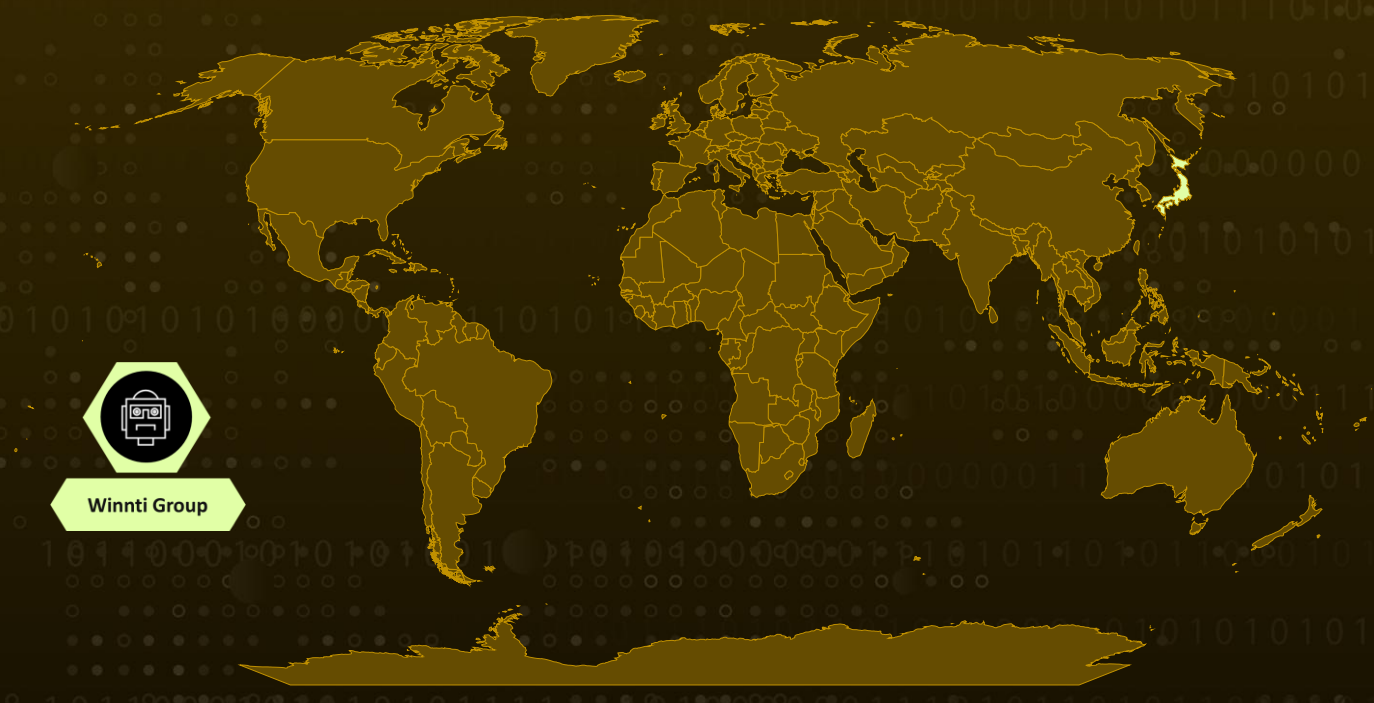
RevivalStone A New Wave of Winnti Group's Cyber Attacks Hits Japan

Date of Publication	Admiralty Code	TA Number
February 20, 2025	A1	TA2025052

Summary

Attack Commenced: March 2024
Malware: Winnti RAT (aka DEPLOYLOG), Winnti Loader (also known as PRIVATELOG), Winnti Rootkit
Campaign: RevivalStone
Threat Actor: Winnti Group (aka APT 41, Blackfly, Wicked Panda)
Targeted Region: Japan
Targeted Industries: Manufacturing, Materials, Energy
Attack: In March 2024, a sophisticated cyber-attack campaign, dubbed RevivalStone, targeted Japanese companies, marking another high-profile operation by the notorious China-based Winnti Group. Leveraging advanced malware and stealthy intrusion techniques, the attackers infiltrated corporate networks, expanding their reach through interconnected systems and leaving a trail of compromised infrastructure.

Attack Regions



Attack Details

#1 In March 2024, a sophisticated cyber-attack campaign, codenamed RevivalStone, was launched by the China-based threat actor known as the Winnti Group. Renowned for its long-standing focus on the gaming industry since around 2010, the group expanded its scope in this operation, targeting Japanese corporations with an enhanced version of its notorious Winnti malware.

#2 The hallmark of the Winnti Group's attacks lies in its use of malware equipped with a specialized rootkit, designed to stealthily manipulate and conceal network communications. Compounding the threat, the attackers employ stolen, legitimate digital certificates to give their malicious software an appearance of authenticity, allowing it to bypass standard security measures.

#3 The RevivalStone campaign began with the exploitation of an SQL injection vulnerability in the ERP system hosted on the target organization's web server. Leveraging this flaw, the attackers implanted a WebShell, granting them remote access to the compromised server.

#4 Through this foothold, they conducted reconnaissance, harvested credentials, and prepared for lateral movement within the victim's network. Soon after, the Winnti malware was deployed onto the server, solidifying the attackers' presence.

#5 At the core of this campaign was the Winnti Remote Access Trojan (RAT) also known as DEPLOYLOG which was executed via the Winnti Loader. Uniquely, the RAT was encrypted and stored within a disguised DAT file which when decrypted revealed a malicious 64-bit DLL file primed for exploitation.

#6 As the intrusion deepened, the attackers escalated their reach by compromising a shared account belonging to an external operations and maintenance company. This credential theft enabled them to move laterally into the network of an infrastructure provider, broadening their access and amplifying the impact. Consequently, multiple organizations relying on this infrastructure suffered collateral damage, with their servers becoming new nodes in the spreading breach.

Recommendations

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to detect suspicious activities, such as unauthorized registry changes, process injections, and the creation of persistent tasks. Ensure rapid response and containment capabilities to neutralize threats as they occur.

Advanced Web Application Firewalls (WAF): Deploy and fine-tune a WAF with anomaly detection capabilities to identify and block complex attack patterns, including WebShell deployments.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
T1190 Exploit Public-Facing Application	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1505** Server Software Component	**T1505.003** Web Shell	**T1574** Hijack Execution Flow
T1574.001 DLL Search Order Hijacking	**T1547** Boot or Logon Autostart Execution	**T1547.006** Kernel Modules and Extensions	**T1543** Create or Modify System Process
T1543.003 Windows Service	**T1078** Valid Accounts	**T1078.002** Domain Accounts	**T1014** Rootkit

T1036 Masquerading	**T1036.005** Match Legitimate Name or Location	**T1070** Indicator Removal	**T1070.004** File Deletion
T1016 System Network Configuration Discovery	**T1018** Remote System Discovery	**T1201** Password Policy Discovery	**T1069** Permission Groups Discovery
T1135 Network Share Discovery	**T1007** System Service Discovery	**T1049** System Network Connections Discovery	**T1033** System Owner/User Discovery
T1082 System Information Discovery	**T1120** Peripheral Device Discovery	**T1021** Remote Services	**T1021.001** Remote Desktop Protocol
T1021.002 SMB/Windows Admin Shares	**T1560** Archive Collected Data	**T1560.001** Archive via Utility	**T1588.004** Digital Certificates

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596, c649e75483dd0883de2fef001a44263a272c6b49a8d1c9ea7c00c044495200ad, 569c1d9b2822c17e64214421409c5649eafc5df9abd88d40a5554f57f32588e8, 169d35bdb36c2bfcb3bbf64392de1b05d56553172a13cae43a43acbe2aa18587, b9d4ec771a79f53a330b29ed17f719dac81a4bfe11caf0eac0efacd19d14d090, 4608a63c039975fb8f3ffd221ec6877078542def44767f50447db1d514eb0779, 1e53559e6be1f941df1a1508bba5bb9763aedba23f946294ce5d92646877b40c

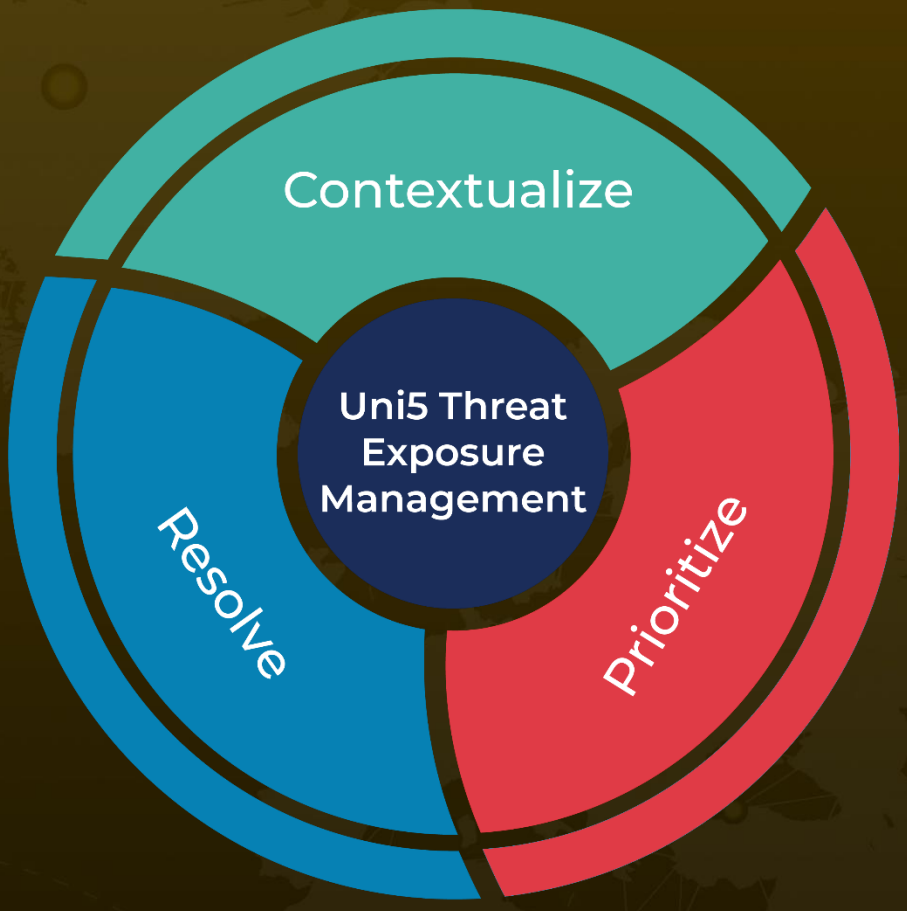
References

https://www.lac.co.jp/lacwatch/report/20250213_004283.html

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

February 20, 2025 • 8:00 PM

More at www.hivepro.com