Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

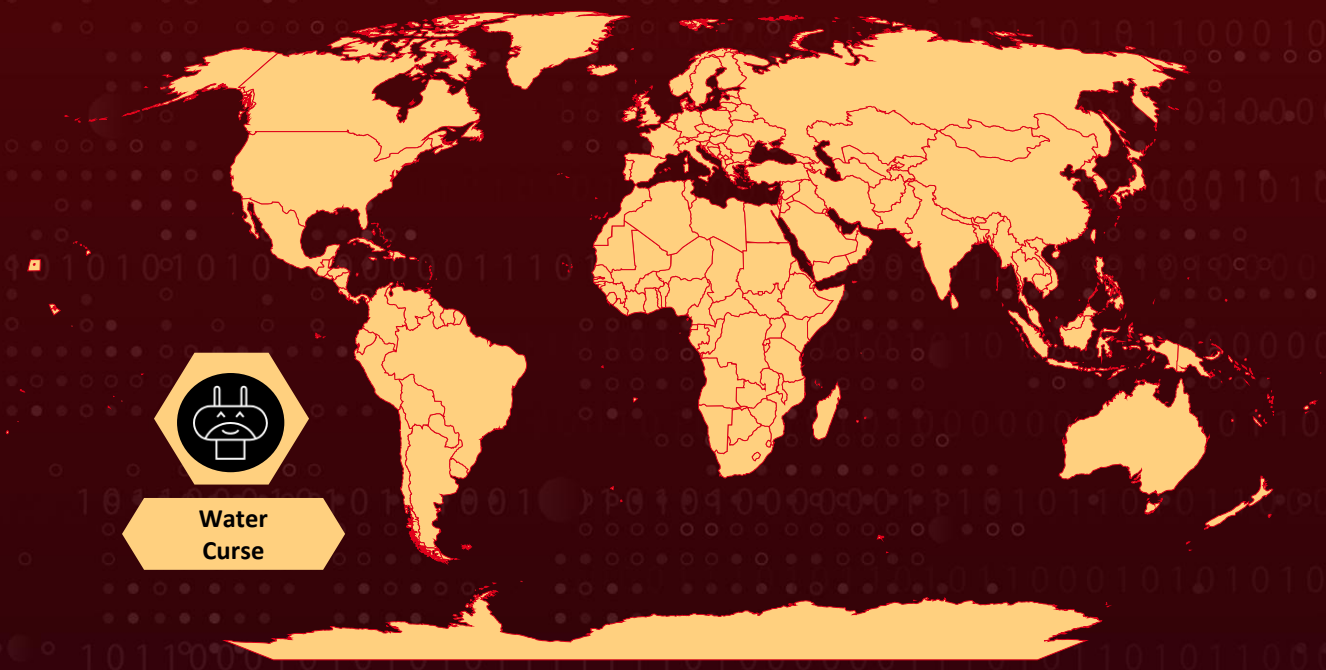
Water Curse Group Weaponizes GitHub Repositories

Date of Publication	Admiralty Code	TA Number
June 18, 2025	A1	TA2025191

Summary

Attack Commenced: May 2025
Targeted Countries: Worldwide
Malware: Sakura RAT, DULLRAT
Targeted Platforms: Windows
Targeted Industries: Cryptocurrency, Gaming, Information Technology
Attack: Water Curse is a financially motivated threat group that weaponizes GitHub by hosting malicious repositories posing as legitimate developer tools. Once cloned and built, these projects execute obfuscated scripts that download and deploy multi-stage malware. The attack chain includes system recon, credential theft, privilege escalation, and persistence, with data exfiltrated via Telegram or public hosts. This campaign targets developers, security professionals, and crypto users through compromised open-source workflows.

Attack Regions



Attack Details

#1

Water Curse is a financially motivated cybercriminal group first observed in March 2023, with a notable surge in activity during May 2025. The group has weaponized at least 76 GitHub accounts to distribute malicious open-source repositories. These repositories pose as legitimate tools, such as penetration-testing frameworks, game cheats, crypto utilities, and email bombers, but conceal multi-stage malware in their build scripts and Visual Studio project files.

#2

Once a user clones and builds one of these repositories, an obfuscated VBScript or PowerShell loader activates. The loader downloads encrypted payloads, including Electron apps, then performs system reconnaissance, disables security features, and escalates privileges. The threat actor achieves stealth and long-term access through scheduled tasks, registry persistence, binary injection, and anti-debugging techniques.

#3

Water Curse's malware is designed to steal credentials (such as browser cookies, saved passwords, and session tokens) and provide remote access to compromised systems. Stolen data is exfiltrated through Telegram bots and public file-hosting services like Gofile and Anonfiles. The group's toolkit includes a variety of payloads, from Sakura-RAT and SMTP bombers to wallet stealers and spam bots, reflecting a broad monetization strategy.

#4

This campaign exemplifies a high-risk software supply chain attack. By exploiting trust in GitHub and hijacking legitimate development workflows, Water Curse poses a threat to cybersecurity professionals, DevOps engineers, game developers, and anyone relying on open-source utilities.

Recommendations

Audit Open-Source Dependencies: Only clone repositories from verified, trusted authors or organizations. Carefully review all scripts—especially build configurations like .csproj, .ps1, or .vbs—before executing or compiling them.

Isolate Build Environments: Conduct all builds of untrusted or unfamiliar open-source projects in sandboxed or containerized environments. This helps detect and contain malicious behavior without exposing production or development machines.

Enable Endpoint Protection and EDR/XDR Tools: Deploy modern Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions. Ensure they are configured to detect script-based threats, registry modifications, privilege escalation, and persistence mechanisms.

Use Internal Repositories: Where feasible, maintain internal mirrors of trusted open-source tools to reduce supply chain exposure.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0010 Exfiltration	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	T1053.005 Scheduled Task	T1119 Automated Collection
T1560 Archive Collected Data	T1102.002 Bidirectional Communication	T1102 Web Service	T1557 Adversary-in-the-Middle
T1497 Virtualization/Sandbox Evasion	T1113 Screen Capture	T1555 Credentials from Password Stores	T1082 System Information Discovery

T1497.001 System Checks	T1213 Data from Information Repositories	T1555.003 Credentials from Web Browsers	T1005 Data from Local System
T1543 Create or Modify System Process	T1036 Masquerading	T1218 System Binary Proxy Execution	T1048 Exfiltration Over Alternative Protocol
T1548 Abuse Elevation Control Mechanism	T1112 Modify Registry	T1027 Obfuscated Files or Information	T1057 Process Discovery
T1548.002 Bypass User Account Control	T1562.001 Disable or Modify Tools	T1562.004 Disable or Modify System Firewall	T1562 Impair Defenses
T1195 Supply Chain Compromise	T1195.002 Compromise Software Supply Chain	T1059.007 JavaScript	T1059 Command and Scripting Interpreter
T1129 Shared Modules	T1059.001 PowerShell		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	6b78948f441eee53f21791d4dd88dd4fdcd5f7e3, 4c189405d684eb8e70b1848b356967e783b9c543, 5cd53d94caf0e811b82bad958b34322eb082567f, e1a02b787597a844b82a73c2488000088d0533b4, ad25ee224973140d41c6ecf1c1500d4efeb0b324, 27c4161777ba005166156de311ba58de49eac874, 435e74551890b8c70c4b09446ec6ce0a932763f5, 4c391ebeff4cdfbc87ca83772a535d4386e5a5b2, 585b76875aad1c99d3e06c29ad46b3adeb45639d, fdb9fc2de72be71084cc60508d00bedbf9337172, 60bdf425bd22c34bad7d5663db31d2107153f729, 68911ad6696cfdb15c967a82c2d8aab1be634659, d94f476b2aceaf4e83197475280f89ecbe3b8d35

TYPE	VALUE
URLs	hxxps[://]rlim[.]com/seraswodinsx/raw, hxxps[://]pastebin[.]com/raw/LC0H4rhJ, hxxps[://]pastejustit[.]com/raw/tfauzcl5xj, hxxps[://]github[.]com/unheard44/fluid_bean/releases/download/releases/SearchFilter[.]7z, hxxps[://]popcorn-soft[.]glitch[.]me/popcornsoft[.]me,
IPv4	46[.]101[.]236[.]176

References

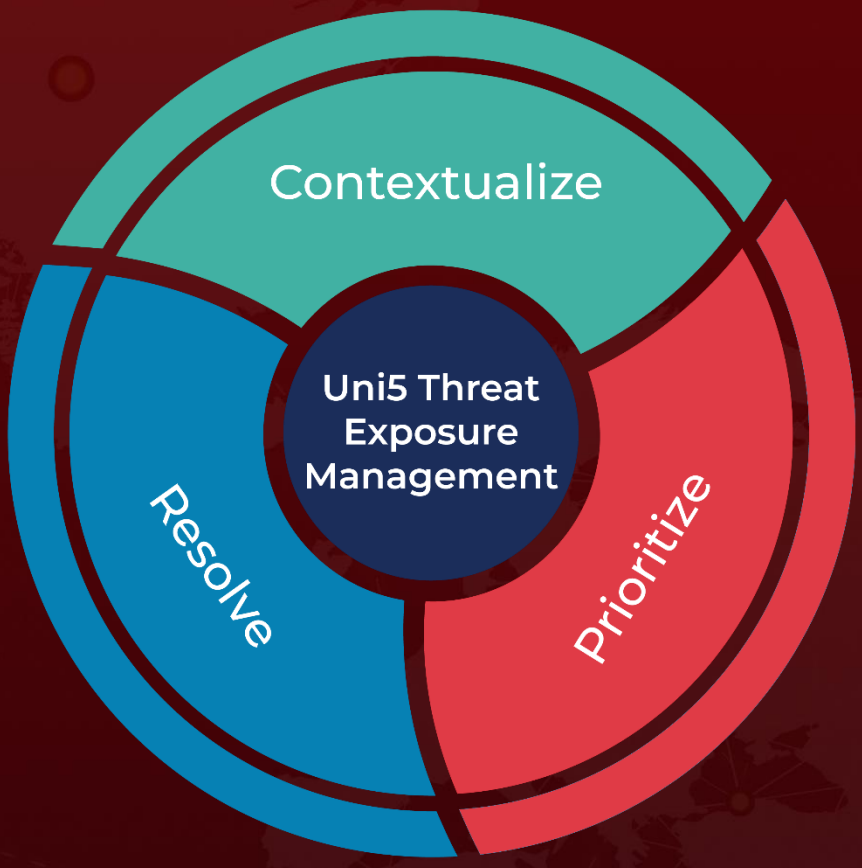
https://www.trendmicro.com/en_us/research/25/f/water-curse.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/25/f/clone-compile-compromise-water-curses-open-source-malware-trap-on-github/Water-Curse-IOCs.txt

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

June 18, 2025 • 2:30 AM

More at www.hivepro.com