Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

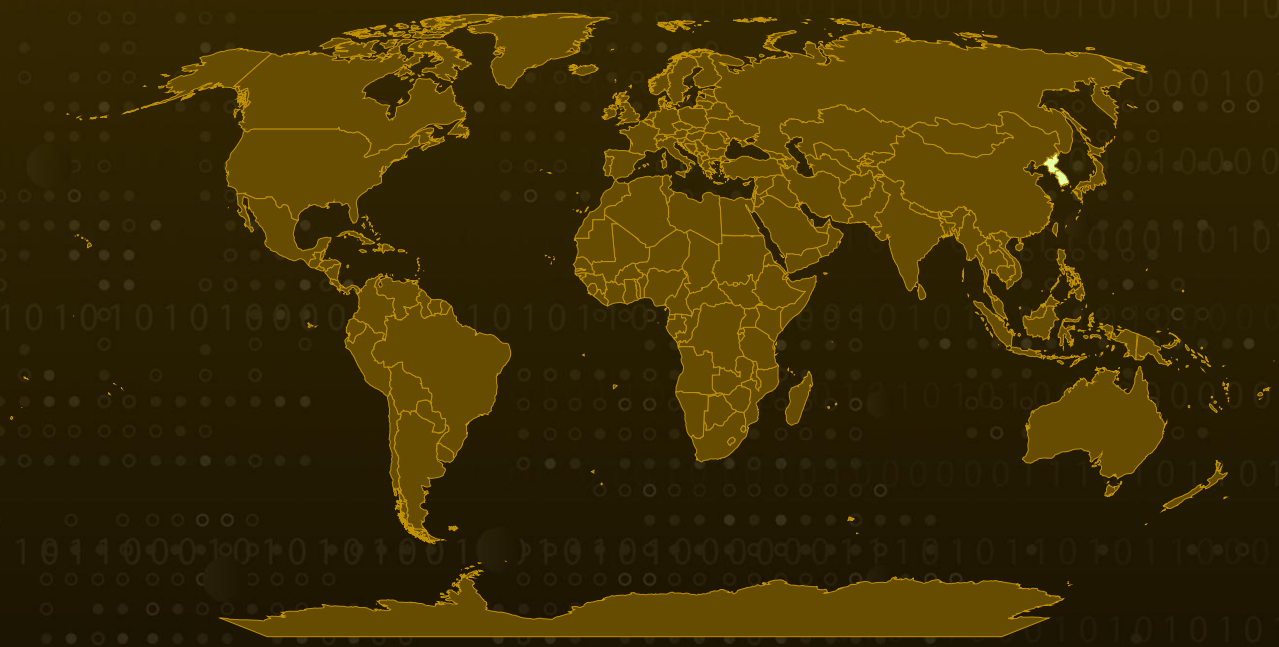
# Threat Actors Turn RMM Tools into Backdoor Gateways

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| November 14, 2025 | A1 | TA2025347 |

# Summary

**Attack Discovered:** 2025
**Targeted Countries:** Korea
**Malware:** PatoRAT
**Attack:** A recent wave of attacks is using fake software download pages to quietly install manipulated versions of LogMeIn Resolve and PDQ Connect, giving attackers remote access to victims' systems. Once inside, they use these trusted IT tools to run commands and deploy PatoRAT, a stealthy backdoor capable of data theft and full device control. The malware's clever disguise, simple encryption, and use of legitimate platforms make it difficult to spot, turning everyday downloads into hidden entry points for attackers.

## Attack Regions



# Attack Details

**#1** Recent attacks have increasingly taken advantage of Remote Monitoring and Management (RMM) tools, particularly LogMeIn Resolve (GoTo Resolve) and PDQ Connect. Although the exact initial infection vector is still unclear, investigators have found that the malware is distributed through fake websites impersonating popular utility software. Unsuspecting users believe they are downloading legitimate tools, such as Notepad++ or 7-Zip, but instead install a maliciously altered version of LogMeIn Resolve bundled with an additional data-stealing payload. In many cases, the threat actors rebrand LogMeIn under multiple misleading names to further trick victims.

**#2** LogMeIn Resolve is a trusted RMM platform used for remote support, patch deployment, and endpoint monitoring. However, its legitimate capabilities can be misused to evade traditional security controls like firewalls and antivirus engines, which often allow RMM tools by default. During recent campaigns observed in Korea, researchers discovered internal configuration files within LogMeIn that exposed the “CompanyId” values tied to the attacker. Three unique identifiers were found, indicating coordinated misuse. Once installed, disguised as harmless freeware, the malicious LogMeIn instance automatically registers within the LogMeIn infrastructure, enabling the threat actor to remotely access the machine, execute PowerShell commands, and deploy additional malware such as PatoRAT.

**#3** Both PDQ Connect and LogMeIn Resolve were abused to push PatoRAT, a Delphi-based backdoor known for enabling remote control and data theft. PDQ Connect, like LogMeIn, provides extensive device management features, including software deployment, patching, inventory tracking, and remote administration. Threat actors leveraged these capabilities to run arbitrary commands silently in the background. This abuse of legitimate RMM platforms helped the attackers bypass detection and establish persistent access through PatoRAT.

**#4** PatoRAT contained internal log messages written in Portuguese and was identifiable through its distinct ClientID. Its configuration was stored in an XOR-encrypted block under the resource tag “APPCONFIG,” using a simple 0xAA key. Once decrypted, the configuration revealed critical parameters: the clientTag, mutex, command-and-control (C2) addresses, and several functional flags. Upon execution, PatoRAT sends initial system information to the C2 server and awaits further instructions, giving attackers full control to execute commands, exfiltrate data, or deploy additional payloads.

**#5** The number of incidents involving backdoor installations through compromised RMM tools continues to rise, underscoring the growing trend of abusing legitimate IT software for malicious purposes.

# Recommendations

- **Download Software Only From Official Sources:** Make sure you're getting applications from their verified websites or trusted app stores. Avoid download links from pop-ups, ads, or unfamiliar sites, even if they look legitimate.
- **Double-check What You're Installing:** Before running any installer, look at the file name, version, and digital certificate. If something feels off, like an unexpected name or a missing signature, don't proceed.
- **Be Cautious With "Free Utility" Downloads:** Attackers often disguise malware as popular free tools (e.g., Notepad++, 7-Zip). If you need such tools, always download them directly from their official websites.
- **Keep Your System and Security Tools Updated:** Regular updates help patch security gaps and give your antivirus the best chance to catch new threats. Turn on automatic updates where possible.
- **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

| | | | |
|---|---|---|---|
| TA0002<br>Execution | TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery |
| TA0009<br>Collection | TA0010<br>Exfiltration | TA0011<br>Command and Control | T1036<br>Masquerading |
| T1219<br>Remote Access Tools | T1204<br>User Execution | T1059<br>Command and Scripting Interpreter | T1059.001<br>PowerShell |
| T1027<br>Obfuscated Files or Information | T1140<br>Deobfuscate/Decode Files or Information | T1082<br>System Information Discovery | T1614<br>System Location Discovery |

| | | | |
|---|---|---|---|
| **T1033**<br>System Owner/User Discovery | **T1056**<br>Input Capture | **T1056.001**<br>Keylogging | **T1113**<br>Screen Capture |
| **T1555**<br>Credentials from Password Stores | **T1555.003**<br>Credentials from Web Browsers | **T1041**<br>Exfiltration Over C2 Channel | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | 04547ab017b84bc1934b39513fd8bad2, 082823d138f9da9b085be91161c3cd04, 17f1080ba64740c0b218e76b0bddb1e2, 2638281ba875fce2fb2f595a7e8cf1fa, 299b22f03a0affcb1ed74889c0c7e436 |
| URLs | hxxps[:]//bithumb-19-10[.]netlify[.]app/%EB%B9%97%EC%8D%B8[.]exe, hxxps[:]//chatg31-10[.]netlify[.]app/chatgpt[.]exe, hxxps[:]//chatgpt-30-10[.]netlify[.]app/ChatGpt[.]exe, hxxps[:]//dazzling-genie-b16946[.]netlify[.]app/Browser%20Update[.]exe, hxxps[:]//joyful-cajeta-66bmicro[.]netlify[.]app/%EB%A7%88%EC%9D%B4%ED%81%AC%EB%A1%9C%EC%86%8C%ED%94%84%ED%8A%B8[.]EXE |
| Domains | lastdance[.]mysynology[.]net, masterpanel[.]webredirect[.]org, patolino[.]theworkpc[.]com, secondfloor[.]dynuddns[.]com |
| SHA256 | cfef3afccf056917d4798aa605698d7bfdd34418d5baebcb7a1a43274aec4ef2, 9d3108ff2c392bbdc20de6c820ab6d804a414267e75bd6c048bc3ea5efacde7b, 41b85fe30ab72844033130e3732369f274a47935da7adb0b141b1502188a39de, a42ce45d065807468704b02e869ee71b058c2cffa02e4955863b3a7cdd602ea7, a92c547352a9c23acea1de16c82c8b3b0bf91a18b4df4c1c44fc097fef62d6c9 |

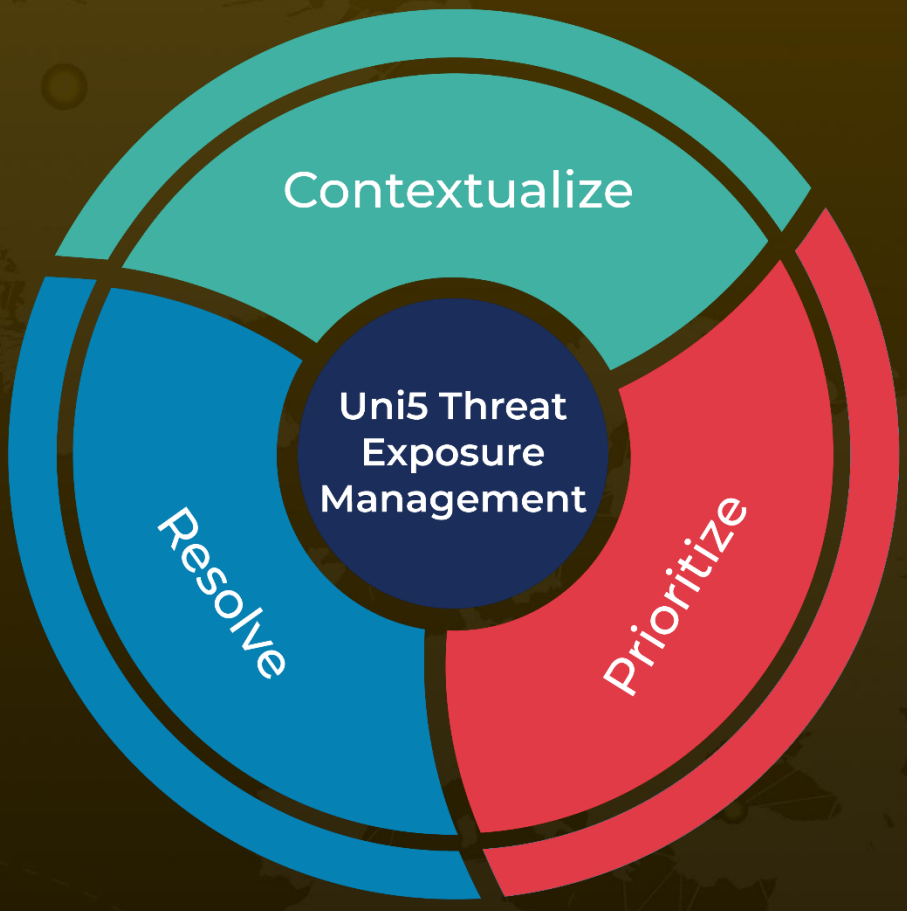
# References

https://asec.ahnlab.com/en/90968/

# 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

**November 14, 2025 . 8:00 AM**



More at www.hivepro.com