Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

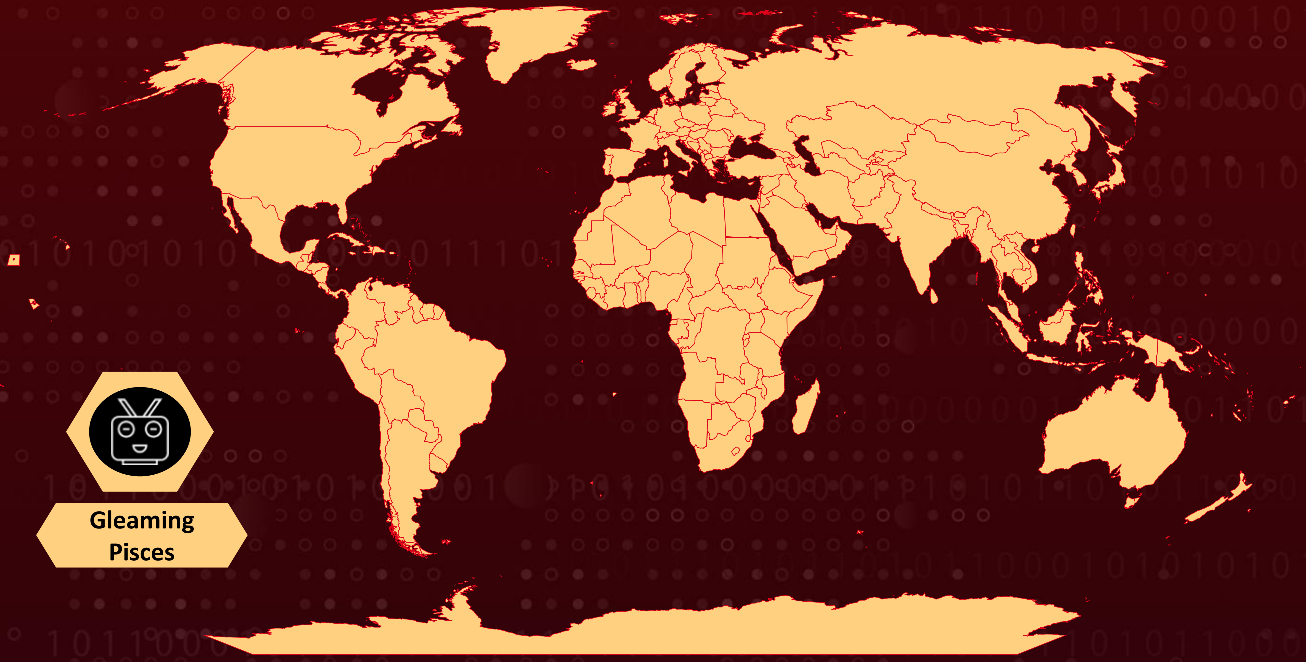
PondRAT Malware Hidden in Python Packages Targets Developers

Date of Publication	Admiralty Code	TA Number
September 24, 2024	A2	TA2024369

Summary

First Appearance: September 2024
Threat actor: Gleaming Pisces (aka Lazarus Group, Citrine Sleet, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)
Malware: PondRAT, POOLRAT
Targeted Region: Worldwide
Affected Platform: Linux and macOS
Attack: PondRAT malware, linked to North Korean hackers, was found hidden in Python packages on PyPI, targeting software developers. It allows remote access to infected machines, posing a serious threat to supply chains by compromising development environments. The malware's similarities to the Gleaming Pisces (aka Lazarus Group) tools highlight increasing risks in the open-source ecosystem. Though the infected packages were removed, the attack underscores the need for stronger security practices in managing third-party code.

Attack Regions



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

Attack Details

#1 The recently discovered PondRAT malware, linked to North Korean threat actors, was found hidden within Python packages on the PyPI repository. This malware targets software developers, allowing attackers to execute remote commands and exfiltrate files. It bears similarities to other Gleaming Pisces (aka Lazarus Group) malware, known for targeting development environments to infiltrate supply chains.

#2 By compromising Python packages, PondRAT poses a significant risk to developer systems, potentially affecting a large number of downstream users. Although the malicious packages have been removed, this incident highlights the vulnerabilities in open-source ecosystems like PyPI, where the extensive use of third-party software can be exploited by attackers. Malicious actors can inject harmful code, putting entire projects at risk.

#3 PondRAT's capabilities, such as remote access to developer machines, uploading/downloading files, and executing arbitrary commands, make it a potent tool for cyber espionage and theft. This type of malware could serve as an entry point to more sensitive networks, particularly if used in large organizations, escalating the damage beyond individual developers. Once embedded in a development environment, it could further taint the software being created or managed on those systems.

#4 Supply chain attacks like this are on the rise, where adversaries compromise the software development process itself to infect end-user products. These attacks target key points in the distribution and development lifecycle, allowing malware to spread more widely once it reaches public-facing applications. Developers are encouraged to follow strict security practices when managing dependencies, such as auditing third-party software regularly and using isolated environments.

Recommendations

Enhance Supply Chain Security: Conduct security audits on third-party vendors to ensure strong cybersecurity practices. Maintain a Software Bill of Materials (SBOM) to track dependencies and detect malicious code. This prevents the integration of compromised libraries into production.

- **Use Trusted Repositories and Verified Packages:** Download packages only from trusted sources like PyPI's Verified Publisher program. Avoid packages with low reputation or unfamiliar authors. Conduct manual code reviews to identify hidden or malicious code early.

- **Implement Strong Endpoint Security:** Deploy endpoint detection tools like Cortex XDR to detect and block malware such as PondRAT. Monitor developer endpoints for unusual activities like unexpected downloads or suspicious network traffic. This helps prevent infection and data breaches.

- **Enhance Network Security:** Segment networks to isolate development environments from critical infrastructure, limiting the impact of a potential compromise. Use Next-Generation Firewalls with advanced threat detection to block malicious domains. This prevents communication with command and control servers.

Potential MITRE ATT&CK TTPs

TA0009 Collection	TA0005 Defense Evasion	TA0001 Initial Access	TA0002 Execution
TA0011 Command and Control	T1070.004 File Deletion	T1070 Indicator Removal	T1195 Supply Chain Compromise
T1222 File and Directory Permissions Modification	T1036 Masquerading	T1059.006 Python	T1059 Command and Scripting Interpreter
T1059.004 Unix Shell	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1213 Data from Information Repositories
T1222.002 Linux and Mac File and Directory Permissions Modification	T1195.001 Compromise Software Dependencies and Development Tools		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c, 0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7, 3c8dbfcbb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e, bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80, bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b, cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86, f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703, 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456
Domains	www[.]talesseries[.]com/write[.]php, rgedist[.]com/sfxl[.]php, jdkgradle[.]com, rebelthumb[.]net

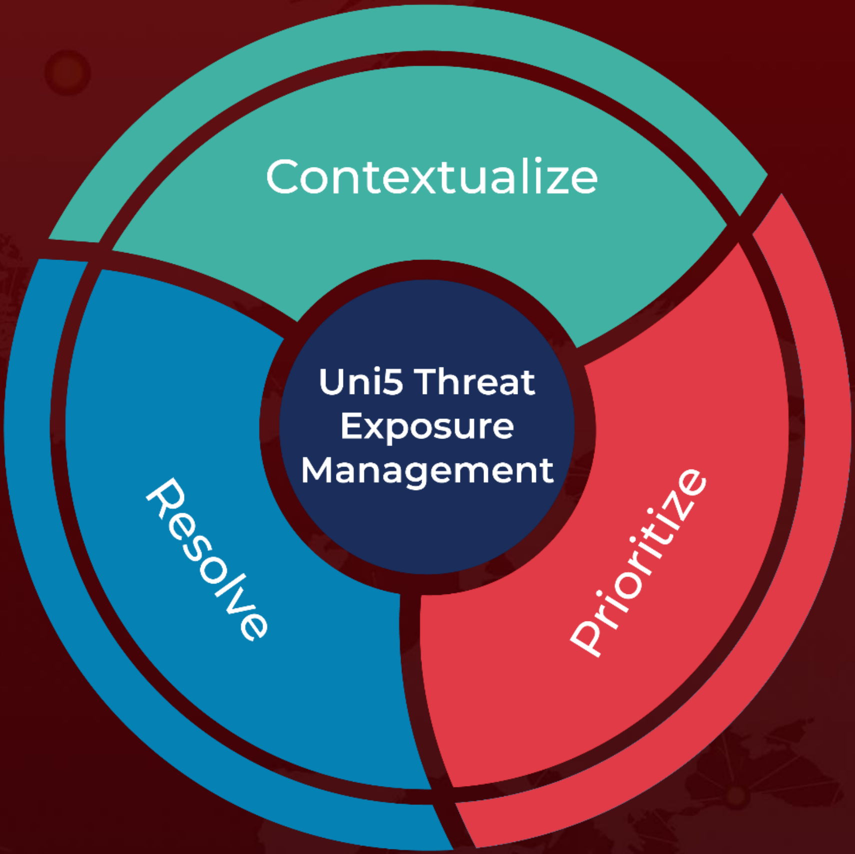
References

https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/?web_view=true

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 24, 2024 • 5:30 AM

More at www.hivepro.com