unit42.paloaltonetworks.com /gleaming-pisces-applejeus-poolrat-and-pondrat/

Gleaming Pisces Poisoned Python Packages Campaign Delivers PondRAT Linux and MacOS Backdoors

Yoav Zemah ⋮⋮ 9/18/2024

Executive Summary

Unit 42 researchers have been tracking the activity of an ongoing poisoned Python packages campaign delivering Linux and macOS backdoors via infected Python software packages. We've named these infected software packages PondRAT. We've also found Linux variants of POOLRAT, a known macOS remote administration tool (RAT) previously attributed to Gleaming Pisces (aka Citrine Sleet, distributor of AppleJeus). Based on our research into both RAT families, we assess that the new PondRAT is a lighter version of POOLRAT.

The attackers behind this campaign uploaded several poisoned Python packages to PyPI, a popular repository of open-source Python packages. We assess with medium confidence that this activity is linked to Gleaming Pisces based on noticeable code similarities, and on previous public research and attribution.

We assess that the threat actor's objective was to secure access to supply chain vendors through developers' endpoints and subsequently gain access to the vendors' customers' endpoints, as observed in previous incidents. A successful installation of third-party packages can result in malware infection, compromising organizations that rely on the popular PyPI repository.

At the time of writing this article, it appears that the PyPI administrators have removed all the poisoned packages referenced in this article.

Through the detection and intelligence provided by **Advanced WildFire**, Palo Alto Networks customers are better protected against PondRAT and POOLRAT through the following products:

- **Cortex XDR** with **Advanced WildFire** can help detect new variants of **PondRAT** and **POOLRAT** and prevent their attack chains.
- **Next-Generation Firewalls** with **Cloud-Delivered Security Services**, including Advanced WildFire detection, **Advanced URL Filtering** and **DNS Security** categorize known command and control (C2) domains and IP addresses as malicious.
- Organizations can also engage the **Unit 42 Incident Response team** to help with a compromise or to provide a proactive assessment to lower your risk.

Related Unit 42 Topics **Python**, North Korea

Gleaming Pisces Overview

Gleaming Pisces (aka Citrine Sleet, distributor of AppleJeus) is a financially motivated threat actor affiliated with North Korea that has been active since at least 2018. This group is closely linked to North Korea's Reconnaissance General Bureau (RGB) and is known for its sophisticated attacks, particularly against the cryptocurrency industry.

Gleaming Pisces gained notoriety for past campaigns where the group deployed fake cryptocurrency trading software to infiltrate and compromise systems across various platforms.

The Connection to Known Gleaming Pisces Malware

During our investigation of the poisoned Python packages campaign described in this writeup, we analyzed the Linux RAT that was delivered as its final payload. We discovered significant similarities with macOS malware used in a previous AppleJeus campaign reported by CISA, orchestrated by the Gleaming Pisces threat actor.

The following similarities indicate a shared codebase:

- Overlapping code structures
- Identical function names and encryption keys
- Similar execution flows

We named this RAT family PondRAT. Further analysis revealed that PondRAT shared many characteristics with POOLRAT, another known macOS RAT in the arsenal of Gleaming Pisces. Based on these findings, we attribute the poisoned Python packages campaign to Gleaming Pisces.

Poisoned Python Packages Campaign Technical Analysis and Detection

While tracking down recent activity by Gleaming Pisces, we came across poisoned Python packages that various malicious fake personas uploaded to PyPI. These poisoned packages implemented an evasive infection chain to

avoid detection and eventually downloaded a Linux RAT onto the infected endpoints. VIPYR Security and Qihoo 360 reported on this activity in detail, specifically involving the following Python packages:

- real-ids (versions 0.0.3 - 0.0.5)
- coloredtxt (version 0.0.2)
- beautifultext (version 0.0.1)
- minisound (version 0.0.2)

Our analysis determined that while Qihoo 360 also reported on Windows-related activities, those activities appear to be separate from the Linux and macOS campaigns. Further, we assess that the activity reported on by Qihoo 360 was performed by a different threat actor, in contrast to the Linux and macOS campaigns that we here connect to Gleaming Pisces.

The infection chain includes several poisoned Python packages that decode and execute encoded code. After Python installed and loaded the malicious package, a malicious piece of code eventually ran several bash commands to download the RAT, modifying its permissions and executing it.

Figure 1 below shows the infection chain and the prevention of PondRAT by Cortex XDR.

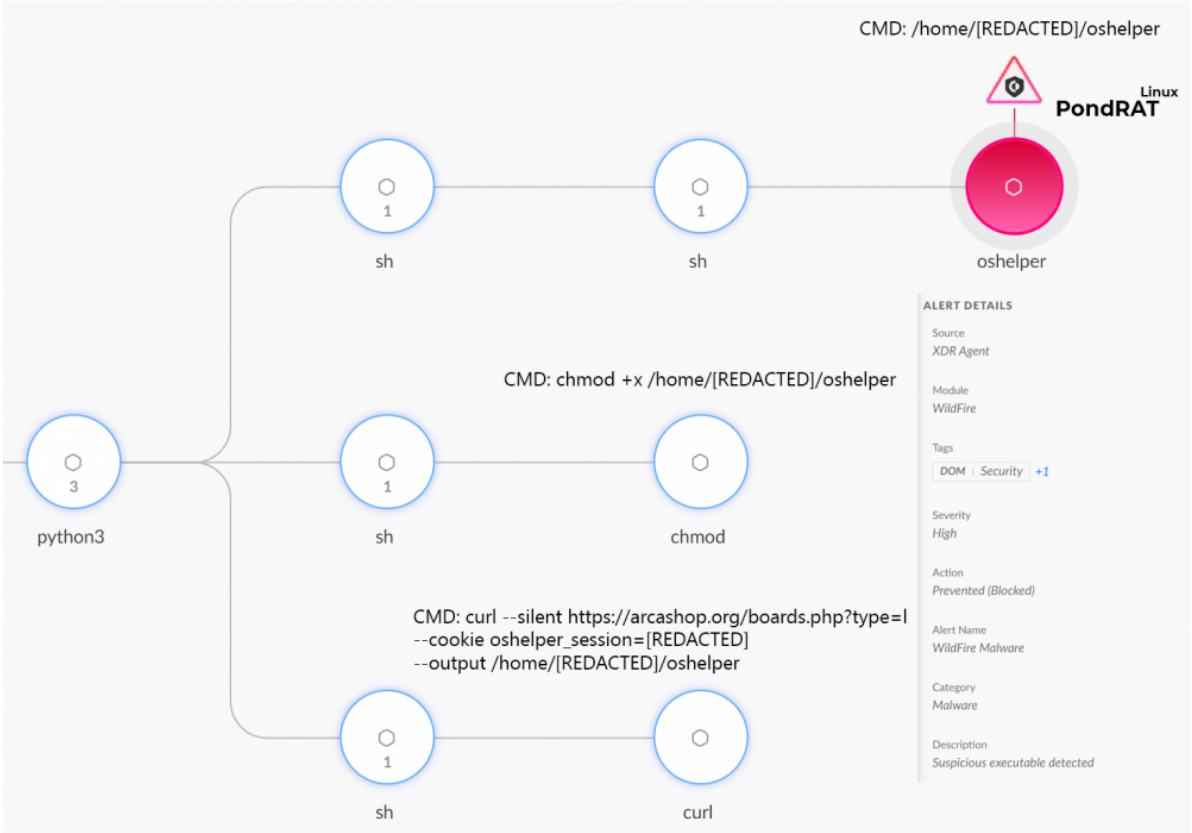

Figure 1. The PondRAT malware prevented by Cortex XDR.

Comparing PondRAT to Previous Gleaming Pisces Attributed Malware

We found other malware by pivoting based on code similarities to PondRAT, as well as to previously conducted research and attribution to Gleaming Pisces. Figure 2 below depicts a summary of these similarities.

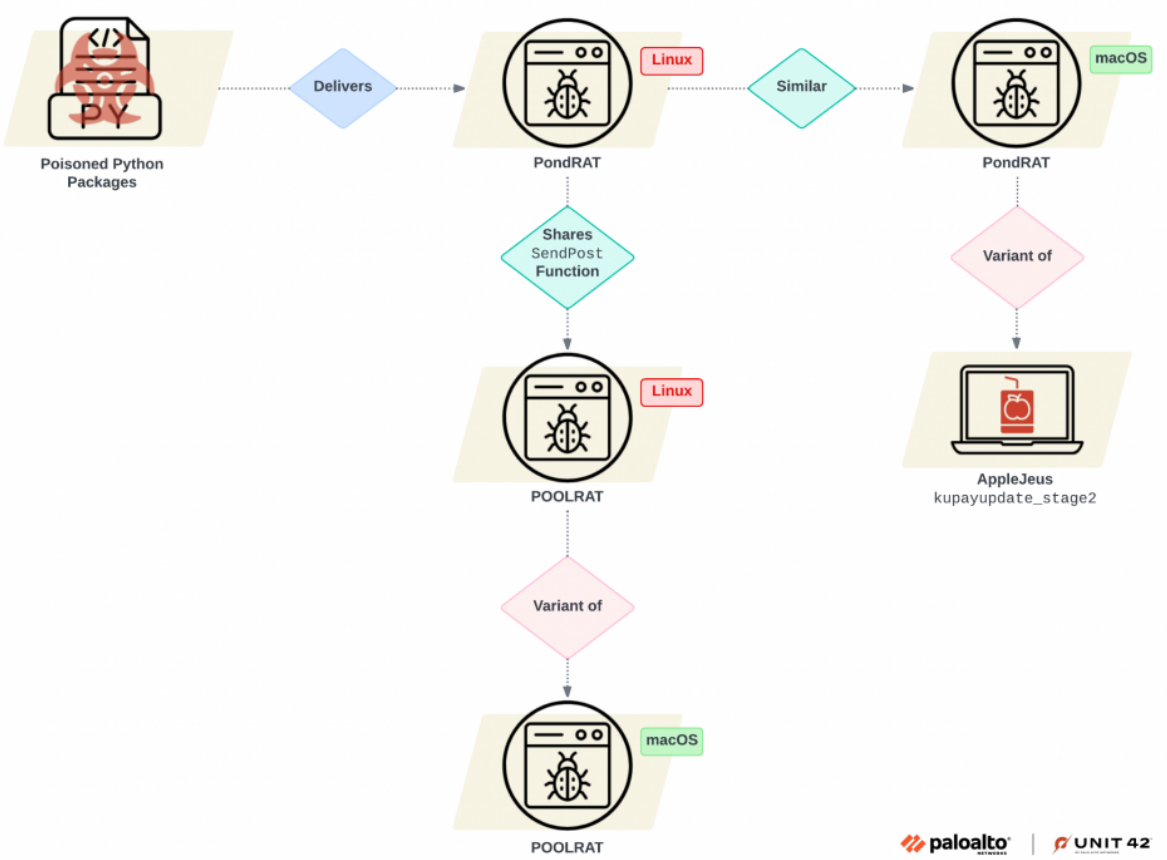

Figure 2. Similarities between the malware we found and other malware previously attributed to Gleaming Pisces.

Code Similarities between PondRAT and Kupayupdate_stage2

In their recently published research, VIPYR Security analyzed the code of a Linux RAT (SHA256: 973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c) that was an unknown at the time, which we now identify as the Linux variant of PondRAT. Gleaming Pisces' operators did not strip the code, meaning the function names remained as the threat actor initially named them.

When we examined this RAT's main function, we saw that it contained calls to two different functions: FConnectProxy and AcceptRequest:

- **FConnectProxy**: This function handles the connection to the C2 server. It sets up the URI and parameters of the HTTP requests.
- **AcceptRequest**: This function parses and decrypts commands from the C2 server and is responsible for receiving and executing commands from their remote operators.

Back in 2021, CISA reported about another AppleJeus attack wave called Kupay Wallet. CISA identified a macOS RAT named kupayupdate_stage2 (SHA256: 91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd) that was used as the final payload of this wave.

Upon analyzing the kupayupdate_stage2 RAT for macOS, we noticed that the malware's functions were also not stripped. When examining its code, we observed several similarities to the Linux RAT. This included the function names FConnectProxy and AcceptRequest, and similar code execution flow.

Figure 3 shows these similarities below.

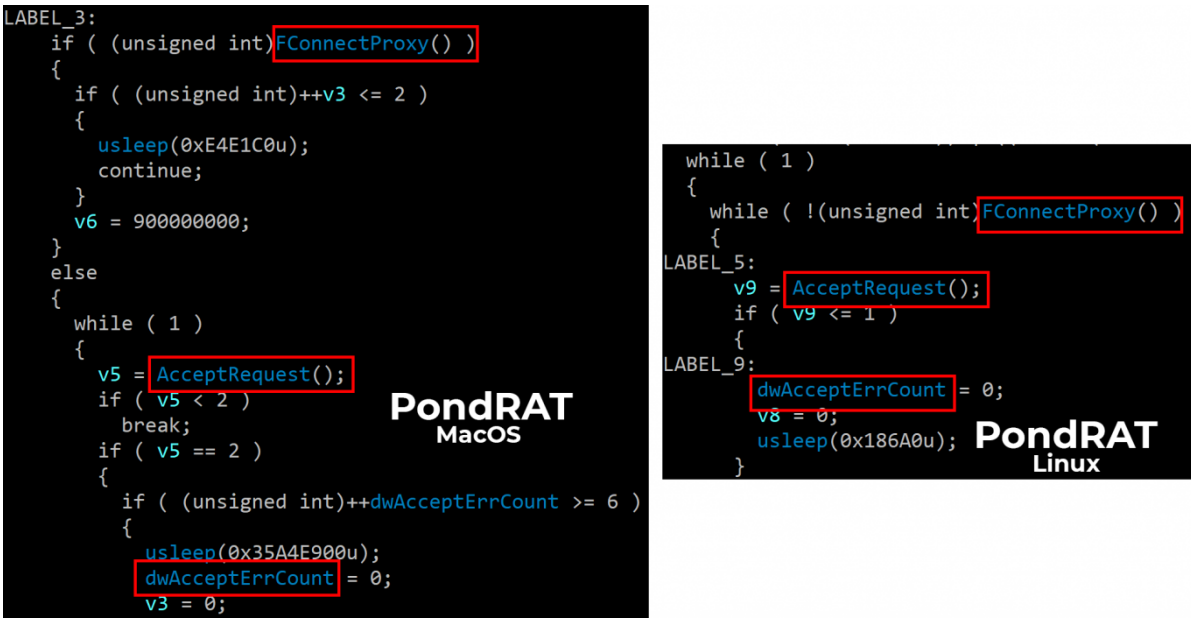

Figure 3. Method names and execution flow similarities of the new Linux RAT and kupayupdate_stage2 RAT.

The next step in our analysis was comparing both of the RATs' AcceptRequest functions. We noticed both variants use the same command numerical IDs and similar method names.

Figure 4 below shows that these functions are almost identical, including the command numerical IDs.

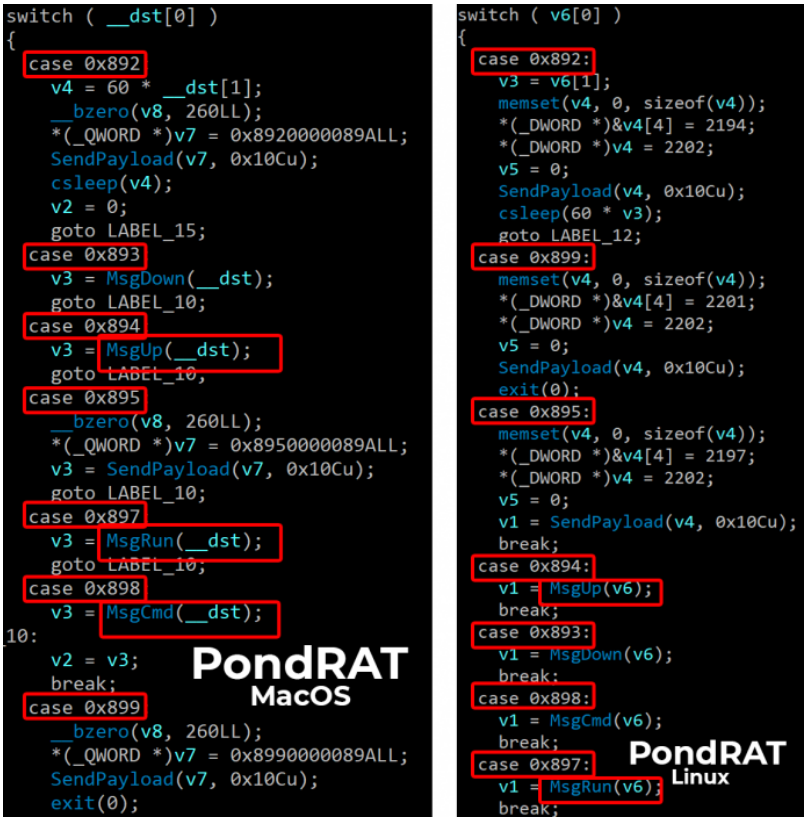

Figure 4. Comparison of both RATs' AcceptRequest function.

Shared Encryption Key

While looking into the encryption method of PondRAT, we noticed that the key used for encrypting output sent back to the server was the following string:

- wLqfM]%wTx`~tUTbw>R^#yG5R(3C:;.

When we compared this key to the one used by kupayupdate_stage2, we noticed it was the same. Figure 5 shows the shared key below.

```
byte_100002B70  db 'w', 'L', 'q', 'f', 'M', ']', '%', 'w', 'T', 'x', '^'
                                        ; DATA XREF: XEncoding(uchar *,uint)+11↑o
                                        ; DecryptPayload(uchar *,uint,uchar *,uint *)+70↑o ...
                db '~', 't', 'U', 'T', 'b', 'w', '>', 'R', '^', 18h, '#'
                db 'y', 'G', '5', 'R', '(', '3', 7Fh, 'C', ':', ';'
```

Figure 5. kupayupdate_stage2 encryption key.

PondRAT MacOS Variants Analysis

Following the aforementioned findings, we pivoted and retrieved additional samples of PondRAT's macOS variant that shared the same encryption key. We found a macOS sample that was previously attributed to be a part of the poisoned Python packages campaign and an additional AppleJeus-related macOS RAT.

os_helper

After analyzing the additional macOS samples that shared the same encryption key, we noticed that one of the samples, a Mach-O multi-arch binary file (SHA256: bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b), was using the same infrastructure as the Linux variant of PondRAT.

Since multi-arch binary files for macOS support both Intel and ARM architectures, this sample contained two other Mach-O binaries. These were compiled for x64 and ARM accordingly, as expected.

The two dropped binaries share the same code (function names and encryption key) with kupayupdate_stage2 as the Linux variant of PondRAT. Based on the apparent code similarities and the shared submitted name os_helper, we assess it was also delivered as the final poisoned Python packages campaign payload. Additionally, these macOS variants used the same C2 (jdkgradle[.]com) as the Linux variant.

Figure 6 below depicts how Cortex XDR prevented the macOS malware execution.

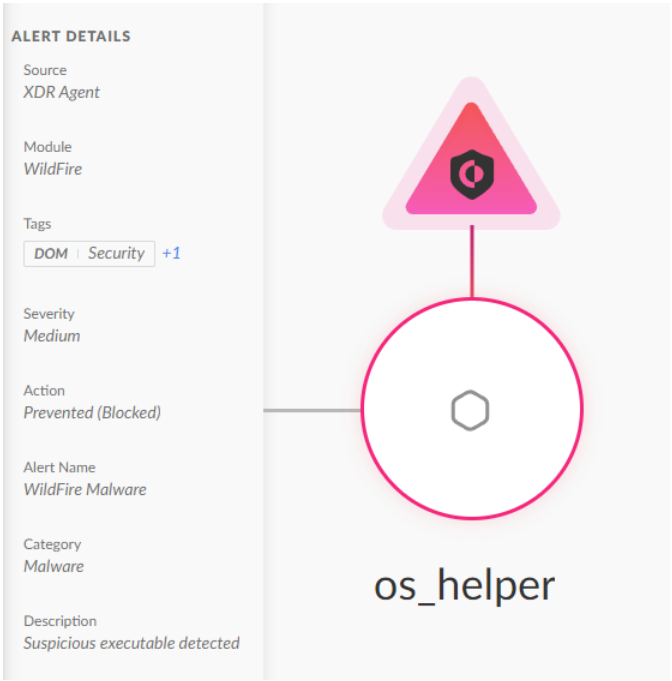

Figure 6. The execution of the os_helper macOS malware prevented by Cortex XDR.

AppleJeus-Related MacOS Variant

Another macOS sample (SHA256: cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86) we found during pivoting that shared the same encryption key was configured to use rebelthumb[.]net as the C2 server. Volexity reported that this domain was part of the AppleJeus campaign back in 2022. This finding further strengthens our attribution of this campaign to Gleaming Pisces.

The Connection between PondRAT and Gleaming Pisces' POOLRAT

During our analysis, we found one more difference between the two PondRAT Linux and macOS variants, aside from being compiled for different OS types. The Linux variant implemented a new SendPost function by using the libcurl library while using the file path /tmp/xweb_log.md as the error log for failed connection attempts to the C2 server.

Searching for files with similar behavior, we identified two more relevant samples that belonged to a Linux RAT exhibiting this trait. We identified this RAT as the Linux variant of POOLRAT.

What Is POOLRAT?

In a 2021 report, CISA identified a macOS RAT dubbed prtspool (SHA256: 5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8), used as the final payload in one of the AppleJeus (CoinGoTrade) attack waves. Mandiant's analysis of the 3CX supply chain attack also mentioned this RAT family. They reported that attackers used the POOLRAT malware to compromise 3CX's macOS build environment.

ESET has also identified similarities between POOLRAT and a backdoor called BADCALL for Linux, also attributed to Gleaming Pisces. Figure 7 below shows the execution prevention of the POOLRAT macOS backdoor.

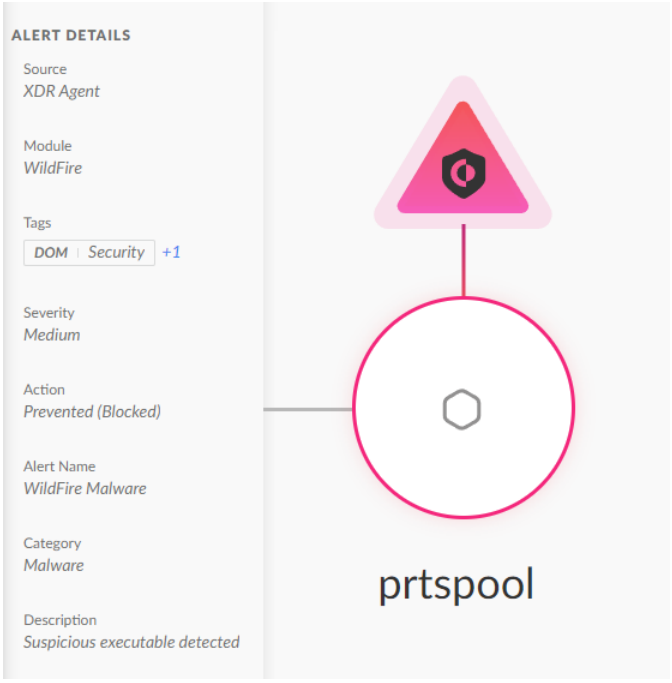

Figure 7. The execution of the POOLRAT macOS malware prevented by Cortex XDR.

The Linux Variants of POOLRAT

The newly discovered Linux variants of POOLRAT (SHA256: 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456, SHA256: f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703) exhibit several notable similarities to its macOS counterpart (prtspool). According to our analysis, we conclude that they are variants of the macOS POOLRAT rather than a new piece of malware.

The Linux and macOS versions use an identical function structure for loading their configurations, featuring similar method names and functionality. Additionally, the method names in both variants are strikingly similar, and the strings are almost identical. Lastly, the mechanism that handles commands from the C2 is nearly identical.

Figure 8 compares the LoadConfig method of POOLRAT's macOS and Linux variants.

Figure 8. Comparison of the LoadConfig function between POOLRAT for macOS and POOLRAT for Linux.

These similarities in configuration and command handling suggest that the Linux versions are adaptations of the original macOS malware, justifying their classification as variants of POOLRAT.

Figure 9 below compares the main functionality of both of the variants.

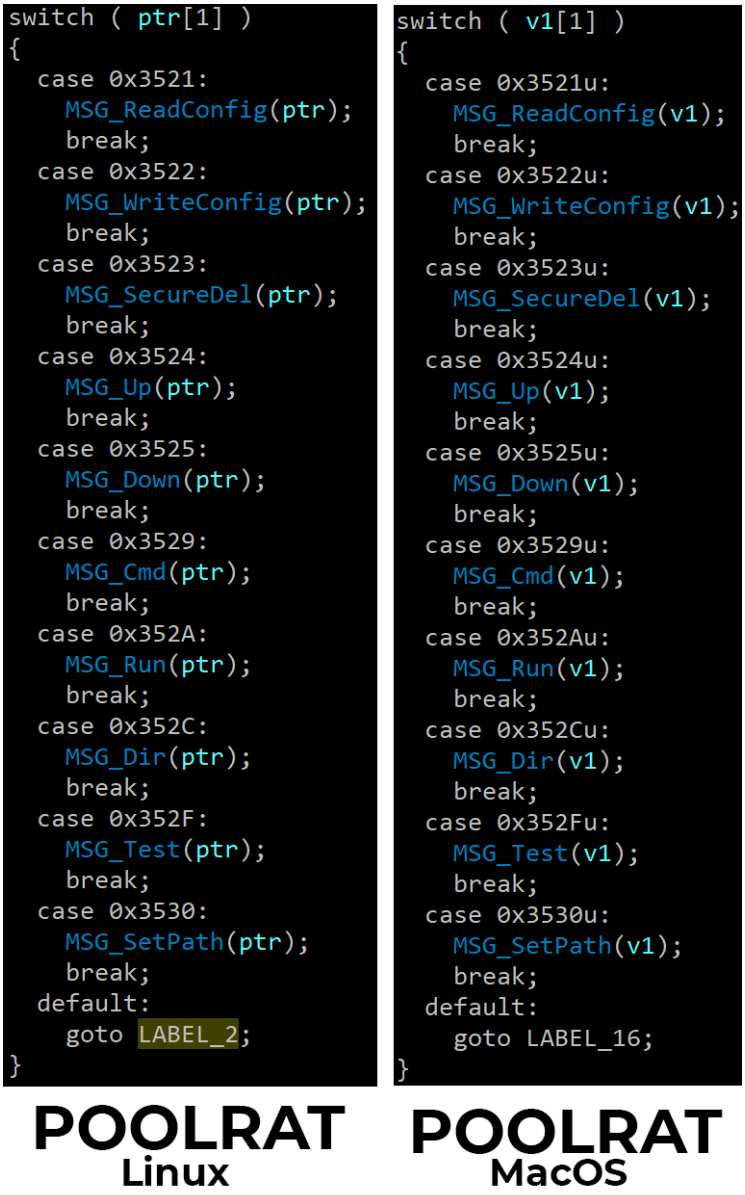

Figure 9. Comparison between POOLRAT for macOS and POOLRAT for Linux.

PondRAT: The Lighter Version of POOLRAT

When analyzing PondRAT samples, we found that the command handler had similarities to POOLRAT.

PondRAT has a straightforward set of commands that give the attacker the following capabilities:

- Uploading and downloading files
- Checking an implant's status to confirm if it is active
- Instructing the implant to pause operations for a specified duration ("sleep")
- Executing commands (with an option to either retrieve their output or not)

As the functionality of PondRAT is similar yet more limited than POOLRAT, we assess that PondRAT is a lighter version of POOLRAT. Table 1 below compares the commands implemented in POOLRAT and PondRAT.

POOLRAT Commands	PondRAT Commands	Description
MSG_Up	MsgUp	Download a file from the C2 server.
MSG_Down	MsgDown	Upload a file to the C2 Server.
MSG_Cmd	MsgCmd	Execute a command and retrieve the output.
MSG_Run	MsgRun	Execute a command and don't retrieve the output.
MSG_ReadConfig		Read the configuration file and send it to the C2.
MSG_WriteConfig		Write a new configuration file.
MSG_SecureDel		Delete a file.

MSG_Dir	List a directory.
MSG_Test	Attempt to connect to an IPv4 address.
MSG_SetPath	Change the current working directory.

Table 1. Comparison between POOLRAT and PondRAT commands.

Conclusion

We've examined the poisoned Python packages campaign and its ties to the North Korean Gleaming Pisces APT group. Our analysis of the Linux variant of PondRAT, which was dropped as the final payload in this campaign, revealed significant similarities to malware attributed to Gleaming Pisces (kupayupdate_stage2).

Furthermore, our investigation uncovered that PondRAT shares code similarities with POOLRAT, malware that was also previously attributed to Gleaming Pisces. The evidence of additional Linux variants of POOLRAT showed that Gleaming Pisces has been enhancing its capabilities across both Linux and macOS platforms.

The weaponization of legitimate-looking Python packages across multiple operating systems poses a significant risk to organizations. Such attacks pose a great risk because they can easily remain under the radar and pose detection challenges. Successful installation of malicious third-party packages can result in malware infection that compromises an entire network.

Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group.

Cortex XDR and **XSIAM** help detect user and credential-based threats by analyzing user activity from multiple data sources, including the following:

- Endpoints
- Network firewalls
- Active Directory
- Identity and access management solutions
- Cloud workloads

Cortex XDR and XSIAM build behavioral profiles of user activity over time with machine learning. By comparing new activity to past activity, peer activity and the expected behavior of the entity, Cortex XDR and XSIAM help detect anomalous activity indicative of credential-based attacks.

Palo Alto Networks also offers the following protections related to the attacks discussed in this post:

- Helps prevent the execution of known malicious malware and execution of unknown malware by using **Behavioral Threat Protection** and machine learning based on the Local Analysis module.
- Cortex XDR Pro and XSIAM help **detect post-exploit activity**, including credential-based attacks, with behavioral analytics.
- **Next-Generation Firewall** with the **Advanced Threat Prevention** security subscription can help block the malware C2 traffic via the following Threat Prevention signature: 86805.
- The **Advanced WildFire** machine learning models and analysis techniques have been reviewed and updated in light of these new PondRAT and POOLRAT variants. Multiple products in the Palo Alto Networks portfolio leverage Advanced WildFire to provide coverage against both PondRAT and POOLRAT variants and other threats.

If you think you might have been impacted or have an urgent matter, get in touch with the **Unit 42 Incident Response team** or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the **Cyber Threat Alliance**.

Additional Resources

- Threat Assessment: North Korean Threat Groups – Unit 42, Palo Alto Networks

Indicators of Compromise

PondRAT Linux variant

- 973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c

PondRAT macOS variant

- 0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7
- 3c8dbfcbb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e
- bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80
- bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b
- cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86

PondRAT C2s

- jdkgradle[.]com
- rebelthumb[.]net

POOLRAT Linux variant

- f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703
- 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456

POOLRAT C2s

- www.talesseries[.]com/write.php
- rgedist[.]com/sfxl.php