Jumpy Pisces Engages in Play Ransomware

unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

Unit 42 October 30, 2024

Executive Summary

Unit 42 has identified Jumpy Pisces, a North Korean state-sponsored threat group associated with the Reconnaissance General Bureau of the Korean People's Army, as a key player in a recent ransomware incident. Our investigation indicates a likely shift in the group's tactics. We believe with moderate confidence that Jumpy Pisces, or a faction of the group, is now collaborating with the Play ransomware group (Fiddling Scorpius).

This change marks the first observed instance of the group using existing ransomware infrastructure, potentially acting as an initial access broker (IAB) or an affiliate of the Play ransomware group. This shift in their tactics, techniques and procedures (TTPs) signals deeper involvement in the broader ransomware threat landscape.

Jumpy Pisces, also known as Andariel and Onyx Sleet, was historically involved in cyberespionage, financial crime and ransomware attacks. The group was indicted by the U.S Justice Department for deploying custom-developed ransomware, Maui.

We expect their attacks will increasingly target a wide range of victims globally. Network defenders should view Jumpy Pisces activity as a potential precursor to ransomware attacks, not just espionage, underscoring the need for heightened vigilance.

Palo Alto Networks customers are better protected from the threats discussed in this article through the following products:

- Cortex XDR and XSIAM
- Advanced WildFire
- Advanced URL Filtering and Advanced DNS Security

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **Threat Actor Groups, North Korea, Ransomware**

Jumpy Pisces' Intrusion Leads to Play Ransomware

In early September 2024, Unit 42 engaged in incident response services for a client impacted by Play ransomware. Play ransomware was first reported in mid-2022. A closed group we track as Fiddling Scorpius is believed to be operating this threat, for both developing and executing the attacks.

Some suggest that Fiddling Scorpius has transitioned to a ransomware-as-a-service (RaaS) model. However, the group has announced on its Play ransomware leak site that it does not provide a RaaS ecosystem.

During our investigation, we discovered with high confidence that the North Korean state-sponsored threat group Jumpy Pisces gained initial access via a compromised user account in May 2024. Jumpy Pisces carried out lateral movement and maintained persistence by spreading the open-source tool Sliver and their unique custom malware, DTrack, to other hosts via Server Message Block (SMB) protocol.

These remote tools continued to communicate with their command-and-control (C2) server until early September. This ultimately led to the deployment of Play ransomware.

Threat actors had access to the network between May-September 2024. Figure 1 shows an overview of the events from this time frame.

Attack Lifecycle – Timeline of Events

We observed the earliest signs of unauthorized activity at the end of May 2024. A compromised user account accessed a particular host through a firewall device. Partial registry dumps on the host indicate possible use of Impacket's credential harvesting module, secretsdump.py.

Attackers copied files associated with the Sliver and DTrack malware family to various hosts using the compromised account over SMB, with the following commands:

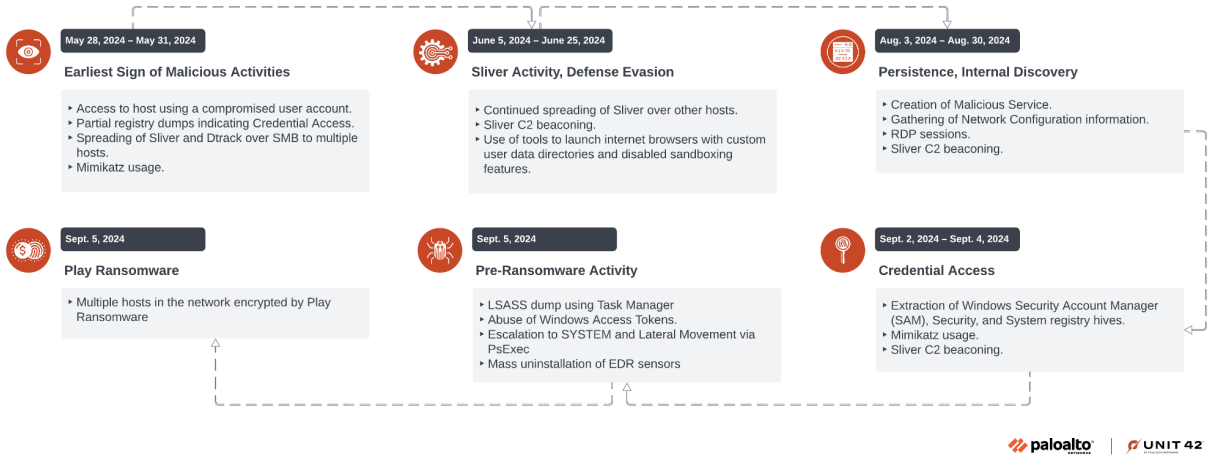

Figure 1. High-level timeline of events.

```
1  cmd /c net use \\<Internal IP>\C$ <Account Password> /user:<Network Domain>\
   <Account Username>
2
3  cmd /c copy <Path to malware> \\<Internal IP>\C$\<Path to malware>
```

DTrack execution was blocked by the endpoint detection and response (EDR) solution. However, we did observe Sliver beaconing activity spanning multiple days until early September 2024, with quiet periods in July and sporadically on other days.

In early September, an unidentified threat actor entered the network through the same compromised user account used by Jumpy Pisces. They carried out pre-ransomware activities including credential harvesting, privilege escalation and the uninstallation of EDR sensors, which eventually led to the deployment of Play ransomware.

Threat Actor Tooling

We observed the following tools and malware during the attack timeline up to the day before the attackers deployed the ransomware. Note that some of the suspicious files observed did not successfully execute, or were not recoverable at the time of investigation.

- Sliver: Attackers used a customized version of the open-source, red-teaming tool for C2 purposes. This tool is often seen as an alternative to Cobalt Strike. This customized version beacons to the IP address 172.96.137[.]224. This IP address has been flagged as a Sliver C2. Both the IP address and the corresponding domain americajobmail[.]site have been linked to Jumpy Pisces.
- DTrack: This is an infostealer previously used in reported incidents attributed to North Korean threat groups. The data it collects is compressed and disguised as a GIF file.

- Attackers used a dedicated tool built to create a privileged user account on victim machines with Remote Desktop Protocol (RDP) enabled.
- Mimikatz: Attackers used a customized version of the publicly available credential dumping tool, with C:\windows\temp\KB0722.log as its credential dump log.
- Attackers used a trojanized binary that steals browser history, autofills and credit card details for Chrome, Edge and Brave internet browsers. The scraped information is saved in a file in %TEMP% directory.

All the above-mentioned files were signed using a couple of invalid certificates that we note in the Indicators of Compromise section of this article. These certificates, previously linked to Jumpy Pisces, enabled the files to impersonate ones created by legitimate entities.

Assessment of Jumpy Pisces – Play Ransomware Collaboration

We assess with moderate confidence a degree of collaboration between Jumpy Pisces and Play Ransomware in this incident, based on the following factors:

- The compromised account that attackers used for initial access and subsequent spreading of the Jumpy Pisces-linked toolset (e.g., Sliver and DTrack), was the same one used prior to ransomware deployment. The ransomware actor leveraged the account to abuse Windows access tokens, move laterally and escalate to SYSTEM privileges via PsExec. This eventually led to the mass uninstallation of EDR sensors and the onset of Play ransomware activity.
- As highlighted previously, we observed Sliver C2 communication until the day before ransomware deployment. Furthermore, our research also suggests that the C2 IP address 172.96.137[.]224 has been offline since the day attackers deployed Play ransomware in this incident.
- Adlumin's report on Play ransomware suggests various commonalities in TTPs across multiple attacks they've tracked. One such TTP was the presence of its tools in the folder C:\Users\Public\Music. We observed some tools used prior to ransomware deployment (i.e., TokenPlayer for Windows access token abuse, and PsExec) both located in C:\Users\Public\Music.

Conclusion

It remains unclear whether Jumpy Pisces has officially become an affiliate for Play ransomware or if they acted as an IAB by selling network access to Play ransomware actors. If Play ransomware does not provide a RaaS ecosystem as it claims, Jumpy Pisces might only have acted as an IAB.

Either way, this incident is significant because it marks the first recorded collaboration between the Jumpy Pisces North Korean state-sponsored group and an underground ransomware network. This development could indicate a future trend where North Korean

threat groups will increasingly participate in broader ransomware campaigns, potentially leading to more widespread and damaging attacks globally.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Advanced WildFire cloud-delivered malware analysis service accurately identifies the known samples as malicious.
- Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with this activity as malicious.
- Cortex XDR detects and prevents all samples mentioned in this article.

If you think you might have been compromised 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 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.

Indicators of Compromise

SHA256 Hashes

- 243ad5458706e5c836f8eb88a9f67e136f1fa76ed44868217dc995a8c7d07bf7
- 2b254ae6690c9e37fa7d249e8578ee27393e47db1913816b4982867584be713a
- f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5
- 99e2ebf8cec6a0cea57e591ac1ca56dd5d505c2c3fc8f4c3da8fb8ad49f1527e
- b4f5d37732272f18206242ccd00f6cad9fbfc12fae9173bb69f53fffeba5553f
- b1ac26dac205973cd1288a38265835eda9b9ff2edc6bd7c6cb9dee4891c9b449

Sliver C2 Server Information

- 172.96.137[.]224
- americajobmail[.]site

Code Signing Certificate Details

SHA256 hash:
b4f5d37732272f18206242ccd00f6cad9fbfc12fae9173bb69f53fffeba5553f
Chain: 6e95d94d5d8ed2275559256c5fb5fc6d01da6b46
Issuer: CN=LAMERA CORPORATION LIMITED
NotBefore: 2/10/2022 9:44 PM
NotAfter: 12/31/2039 4:59 PM
Subject: CN=LAMERA CORPORATION LIMITED
Serial: 879fa942f9f097b74fd6f7dabcf1745a
Cert: 6e95d94d5d8ed2275559256c5fb5fc6d01da6b46

SHA256 hash:
f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5
Chain: 6624c7b8faac176d1c1cb10b03e7ee58a4853f91
Issuer: CN=Tableau Software Inc.
NotBefore: 5/27/2023 11:15 AM
NotAfter: 12/31/2039 4:59 PM
Subject: CN=Tableau Software Inc.
Serial: 76cb5d1e6c2b6895428115705d9ac765
Cert: 6624c7b8faac176d1c1cb10b03e7ee58a4853f91

Additional Resources

- Threat Actor Groups Tracked by Palo Alto Networks Unit 42 – Unit 42, Palo Alto Networks
- North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers – U.S. Department of Justice
- PlayCrypt Ransomware-as-a-Service Expands Threat from Script Kiddies and Sophisticated Attackers – Adlumin
- Stonefly: Extortion Attacks Continue Against U.S. Targets – Symantec, Broadcom
- Onyx Sleet uses array of malware to gather intelligence for North Korea – Microsoft
- North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector – Cybersecurity and Infrastructure Security Agency (CISA)
- #StopRansomware: Play Ransomware – Cybersecurity and Infrastructure Security Agency (CISA)
- Andariel deploys DTrack and Maui ransomware – Kaspersky

Tags

- Cobalt Strike
- DPRK
- DTrack
- Fiddling Scorpius

- Infostealer
- Jumpy Pisces
- Mimikatz
- North Korea
- PsExec
- Sliver

Threat Research Center Next: Deceptive Delight: Jailbreak LLMs Through Camouflage and Distraction

Table of Contents