



ThreatCure

Cyber Threat Advisory

Jumpy Pisces

Criminal Threat Actor

Description

JUMPY PISCES

CATEGORY

Criminal Threat Actor

SEVERITY

High

Platforms

Windows, Linux, Cloud Environments, Web Applications, EDR

IMPACT

- Operational Disruption
- Data Breaches
- Economic and Reputational Damage

Jumpy Pisces, a North Korean state-sponsored threat group associated with the Reconnaissance General Bureau of the Korean People's Army, has recently altered its strategies by forming an alliance with the Play ransomware group, also known as Fiddling Scorpius. This development marks a significant first for Jumpy Pisces, as it utilizes established ransomware infrastructure, potentially acting as either an initial access broker or an affiliate of Play. Previously focused on cyberespionage and financial crimes, Jumpy Pisces has faced indictment from the U.S. Justice Department for deploying custom ransomware like Maui. This new emphasis on ransomware indicates a notable shift in their operations, pointing to a deeper involvement in the wider ransomware ecosystem.

In a recent incident, Jumpy Pisces gained access through a compromised user account, enabling them to conduct lateral movement and maintain persistence using tools such as Sliver and DTrack. Their presence in the network lasted from May to September 2024, culminating in the deployment of Play ransomware following credential harvesting and the removal of endpoint detection and response (EDR) solutions. This partnership reflects a troubling trend where North Korean threat groups are increasingly engaging in ransomware activities, which could lead to more extensive and damaging attacks on a global scale. Consequently, cybersecurity professionals should consider Jumpy Pisces's activities as indicators of potential ransomware threats and bolster their defenses against these evolving tactics.



Attack Chain

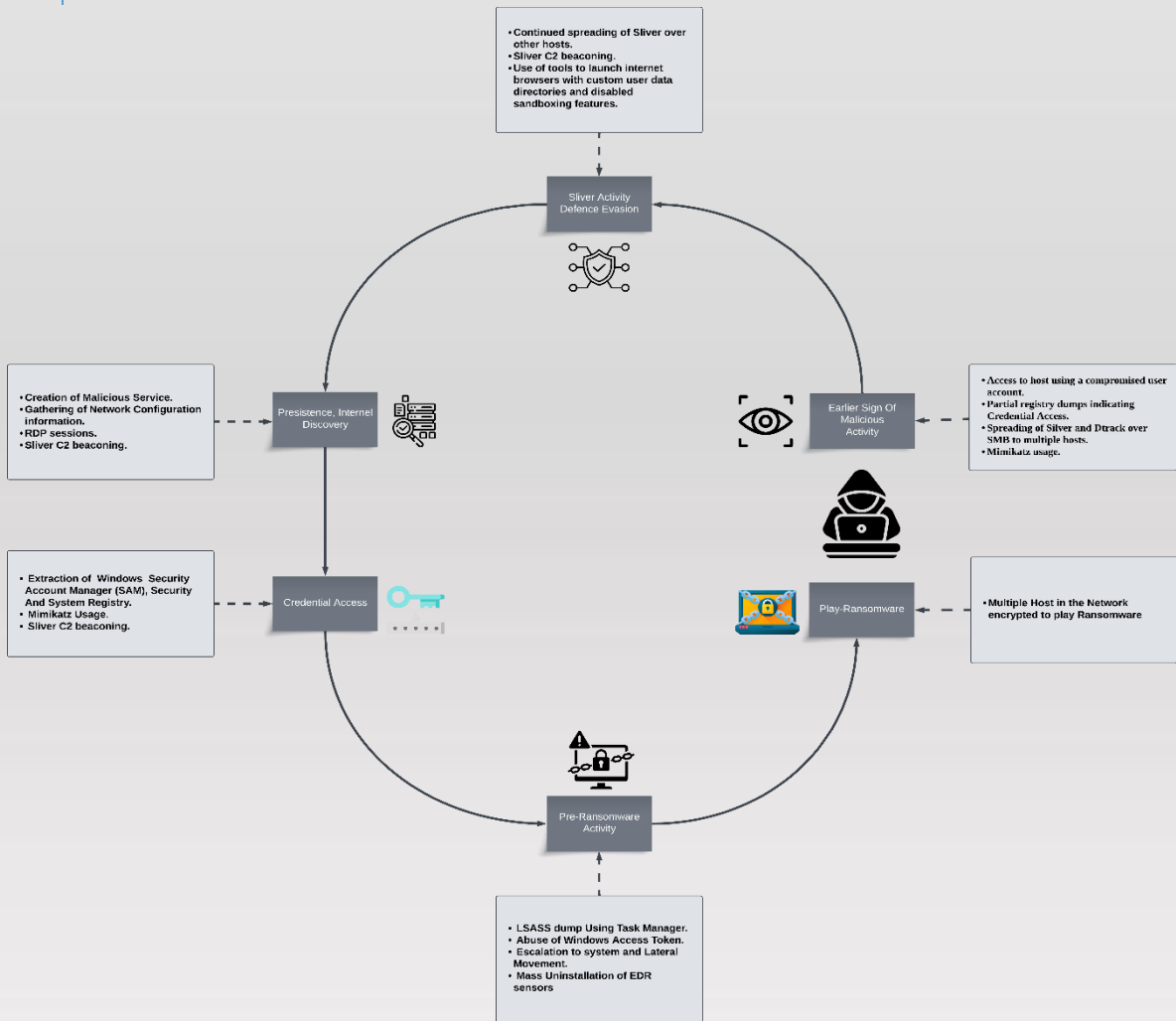


Figure 1 Event sequence summary

Indicator of Compromise

SHA-256

c7f4aa77be7f7afe9d0665d3e705dbf7794bc479bb9c44488c7bf4169f8d14fe
3ea2ead8f3cec030906dcbffe3efd5c5d77d5d375d4a54cca03bfe8a6cb59940
f64dab23c50e3d131abcc1bdbb35ce9d68a34920dd77677730568c24a84411c5
b1ac26dac205973cd1288a38265835eda9b9ff2edc6bd7c6cb9dee4891c9b449
c9a7b42c7b29ca948160f95f017e9e9ae781f3b981ecf6edbac943e52c63ffc8
3ea2ead8f3cec030906dcbffe3efd5c5d77d5d375d4a54cca03bfe8a6cb59940
2360a69e5fd7217e977123c81d3dbb60bf4763a9dae6949bc1900234f7762df1
689cfaa9319f3f7529a31472ecf6b2e0ca6891b736de009e0b6c2ebac958cc94
c6a48365c3db9761bd60981bdcd87aced23d8e60067caa30fee501bf4b47b84
a03d13c9825e150810e6e6aaf053d71ec5a53b86581414dd982a74d4a8bc5475
927b3564c1cf884d2a05e1d7bd24362ce8563a1e9b85be776190ab7f8af192f6
e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
a64fa9f1c76457ecc58402142a8728ce34ccb378c17318b3340083eeb7acc67
479038eb12ed07893ee0dcc04fbdcf182489bbb271f5a4f90f83874881a80ce3
2546d239a262c24a6f8ea01d890cbc459a22db79b379b6ec3b24fbb56efb5381
5009c7d1590c1f8c05827122172583ddf924c53b55a46826abf66da46725505a
87c5d0c93b80acf61d24e7aaf0faae231ab507ca45483ad3d441b5d1acebc43c
99dbc6fe3c3e465052fcef1642861747dc9e069eeb244589b605bd710b1e0d1
fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7
7667d1b8fcc4f712084e3e3f8b4ab505ab150c52aea7b219249ec508b4b0e224
6c121f2b2efa6592c2c22b29218157ec9e63f385e7a1d7425857d603ddef8c59
8bfa4fe0534c0062393b6a2597c3491f7df3bf2eabfe06544c53bdf1f38db6d4
15d53bb839e00405a34a8b690ec181f5555fc4f891b8248ae7fa72bad28315a9
f1713afaf5958bdf3e975ebbab8245a98a84e03f8ce52175ef1568de208116e0
081804b491c70bfa63ecdb9fd4618d3570706ad8b71dba13e234069648e5e48
f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703
5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456
5e40d106977017b1ed235419b1e59ff090e1f43ac57da1bb5d80d66ae53b1df8
973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c
0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7
3c8dbfcb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e
bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80
bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fbd4acf6b
cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86
91eaf215be336eae983d069de16630cc3580e222c427f785e0da312d0692d0fd
c83c7b000a955f2b8cb92bb112ed606ffd9fbebbe3422f80d90d06b167f2f37b
492a643bd1efdaca4ca125ade1b606e7bbf00e995ac9115ac84d1c4c59cb66dd
63fb47c3b4693409ebad8a5179141af5cf45a46d1e98e5f763ca0d7d64fb17c
db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
d8565d58ad8e4f5558b5cd70df0ad12be9cf44e32ad07aaac6f65b816edbf414
243ad5458706e5c836f8eb88a9f67e136f1fa76ed44868217dc995a8c7d07bf7
2b254ae6690c9e37fa7d249e8578ee27393e47db1913816b4982867584be713a
99e2ebf8cec6a0cea57e591ac1ca56dd5d505c2c3fc8f4c3da8fb8ad49f1527

| Remediation

Incident Response Planning: Establish a clear plan detailing how to detect and respond to ransomware incidents.

Preventive Measures: Educate users on security best practices and implement multi-factor authentication to reduce risk.

Network and System Hardening: Regularly update systems, apply patches, and disable unnecessary services to close vulnerabilities.

Monitoring and Detection: Use SIEM tools for continuous monitoring to detect unusual activities early.

Data Backup and Recovery: Maintain secure, regularly tested backups of critical data to facilitate quick recovery.

Incident Containment and Eradication: Isolate affected systems and conduct forensic analysis to understand and eliminate threats.

Communication and Reporting: Keep stakeholders informed and report incidents to law enforcement as necessary.

Post-Incident Review: Analyze the incident to identify lessons learned and update security measures accordingly.



ThreatCure

Cyber Threat Advisory

Secure your byte world



Jumpy Pisces

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

