Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Reaper, North Korean hacking group, targets defectors

Date of Publication

March 20, 2023

Admiralty Code

A1

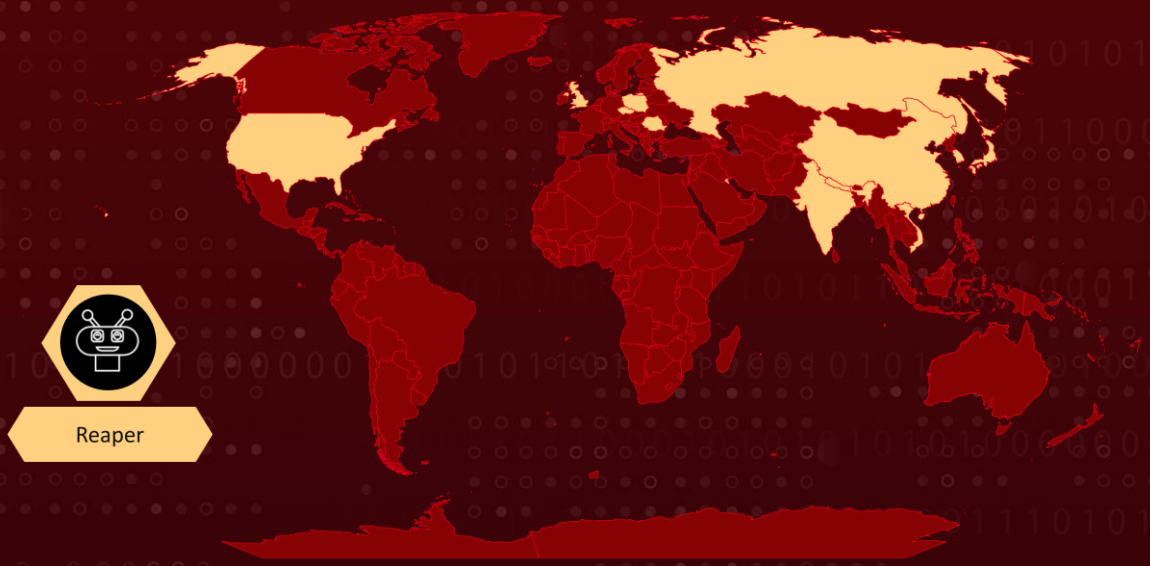
TA Number

TA2023145

Summary

First Seen: 2012
Threat Actor: Reaper (APT 37, Ricochet Chollima, ScarCruft, Thallium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10)
Attack Countries: China, Czech, Hong Kong, India, Japan, Kuwait, Nepal, Poland, Romania, Russia, South Korea, UK, USA, Vietnam
Attack Industry: Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation, Defectors, NGOs
Malware: Chinotto
Attack: North Korea-linked hacking group Reaper has been actively conducting cyber espionage campaigns against NGOs and civil society since at least 2012, and they have recently been observed engaging in surveillance of North Korean defectors.

Attack Regions



Attack Details

#1 According to the investigation, two open directories were discovered on the Command-and-Control servers used by the North Korean-linked hacking group Reaper, also known as APT37. These directories allowed the investigators to view the malicious software that was hosted on the servers as well as the data that had been stolen from the group's victims. The group has been active since at least 2012, primarily conducting cyber espionage campaigns against NGOs and civil society.

#2 The investigation uncovered several interesting findings, including several phishing webpages, a CHM infection vector, new PowerShell implants, and Chinotto malware modules. Chinotto malware is a type of malware that was first documented in November 2021 and has since been associated with the Reaper group. It is noteworthy that the investigation uncovered new PowerShell implants, which are powerful tools used by attackers to carry out malicious activities.

#3 Based on the observed activity, it is highly likely that the group is currently conducting surveillance on North Korean defectors. This activity is associated with high confidence to Reaper, and it is possible that the group is using their cyber espionage capabilities to identify and target defectors.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1212 Exploitation for Credential Access	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1059.005 Visual Basic	T1056 Input Capture	T1056.001 Keylogging	T1113 Screen Capture
T1584 Compromise Infrastructure	T1584.006 Web Services	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1140 Deobfuscate/Decode Files or Information	T1033 System Owner/User Discovery	T1082 System Information Discovery	T1560 Archive Collected Data
T1560.002 Archive via Library	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel
T1573.001 Symmetric Cryptography	T1041 Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp[:]//141.105.65[.]165/data/ hxxp[:]//141.105.65[.]165/files/ hxxp[:]//141.105.65[.]165/main/ hxxp[:]//141.105.65[.]165/support/ hxxp[:]//attiferstudio[.]com/install.bak/sony/ hxxp[:]//ri-guard[.]com/download/temp/cn-var/ hxxp[:]//koaagj.co[.]kr/files/2014/12/fix/ hxxp[:]//jdwanxiang[.]com/win/shenti/ hxxps[:]//clovery-shapes.000webhostapp[.]com/defcon/ hxxp[:]//hk-law.co[.]kr/data/file/joomla/ hxxp[:]//172.93.193[.]158/data/
SHA256	e96a18b5837c7a7d83215d70ca10b84ee8c7b6e8dbd4d215586ec062d328ce86, 1304fbeca197e4e67959c0b89b619cc109e4825d0da26ac41277eb34d2a19bc6, 1409c4d0bd9a22a1e5adf016fffb83bbf3bd9f72ae0773780a409b980ed97763, 6c1f0deadbfe5aede933592a9692b18879232a29bfdda5a666b91475b4746612, c9ea7afef5ac790297bdd0fb78c06186516957542e5da326075a0e2d230c27c1, a320ef003f43b28960043f95076c2066891e3a6a785476a2615a1f7b50a11c78, a88dc9a152cc7758a1df5aa33cf7b31cdb14e593a8744f2059602a49b8b04e0f, 1fcf8bfcd70b97c6d3c9ac93602db4ee41a5d09f0a4b92fa67b76668fb33811d, 309cb38fbcd0132552fc739dd37d32c24b91ba712bebb9886d4638bceb2d8bf3, 001e8e66fa4afc58cab23f5ee490f3080ef985c83d3b2a4555fc9c39cfe56bd8, 3f0f0060bebd891008eaf8a647d91803107fc52294ceaab8b59b89958db4a0de, 58cdb73495c2d6120f81f3752828f532b6a70ce7617b725e6989cf2d9cdb6aa4, 5e67b5aed329e6545a36eff46bb6db8bdaa17841a4ec77228955d81872fed549, ccb6b0e02f7a9d7a541d0ed352706de943c178650a675eff667cb848ec0dc977, c0a36e340cc38c9abd07029e3d621395575c9a4a64459334ef84b623d1058865,

TYPE	VALUE
SHA256	40341da349e684593bbd01b244f94c28aa024ee49c3b3ebc89960e53e40750ae, 9c30265e5b8f7b6017141815001a0678a99d05dc8302b50517c47d5f282b3c36, 575631e9548b0f91addf3ce68bc5b4b9e86a17c069a221815062e1aa93d2978e, cd2028bf873293aa330eb21ab96f8e71fa91e2d212852e81f292e769c0fba2d7, 2a22da882f05dc159b055b01de7331e22fb6b5ce858308015a912b49487c56f0, b4a8d58b5d5e49d9d65b8b9faba344923cbac87473f2a32c646e359799ed655e, 3d6c99e137bf5653134049caf9010d4c6d82360bf569ecca05fe15440d7fd0b0, ff5fc46c9598a5fbc9b54fbbd05ee0bb86549ecbba715093413326b58a1b9d2b, b364bac52981edd74fbc45cca4216e66da5df9918000cc4617156ab42c914e7e, b73ee977154402f8eecc5a446baf0dba456a37d1ca9348858540a8d048f3fd37, 2fa36a4eb676f3afb1774224bc59041944ddfa4a3417630d01659ba3f0ced834, ead97a3920ff557299bcd4ccde1770c759263b93b70414258ec9030bbd0cb750, bdb33062bddd53043bab508e8e96b7c8353549d8eaa4b9004e7b3303e8a4e91b, 0b6202a043f8dcf0690660c5c8f7a75f07336ca5576164295da34a569129548f, 8078fc582b8f5eb81ef5d8da2b11fb4ce63f52fdeb1c2ceb3ac7a01113f9f3ee, 60804ebbb655ea68b9e0bce63d5edbd03e0f75837f44539fec28dc12d44b5ba5, e6d9c5a401a733ceb80b004deb347092affe572eda4e1ca6aa6c77bb0c6ea7e8

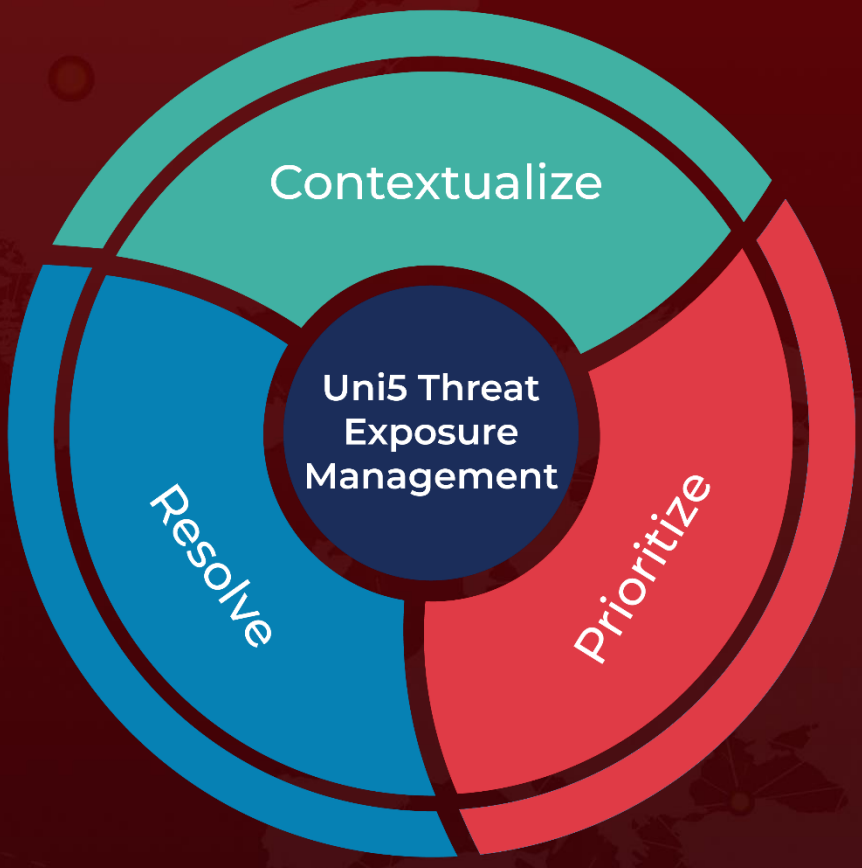
References

https://blog.sekoia.io/peeking-at-reaper-surveillance-operations-against-north-korea-defectors/

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

March 20, 2023 • 5:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com