Report

North Korean State-Sponsored Cyber Attack: Unveiling the Intricacies of Threat Actor Group Andariel

SecurityScorecard threat intelligence research on state-sponsored cyberattacks

SecurityScorecard

SecurityScorecard.com

info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

Introduction

This SecurityScorecard threat research sheds light on a significant cyber attack attributed to North Korean state-sponsored actors known as Andariel, emphasizing the critical role that South Korea plays both as a target and a source of infrastructure for these threat actors.

- **South Korean Defense Contractor Targeted:** Based on details that South Korean authorities revealed in December 2023, SecurityScorecard researchers determined that one likely victim was South Korean defense contractor Hanwha Corporation. South Korean military and defense organizations are top targets for state-sponsored North Korean cyber espionage due to the decades-long hostility and military tensions between the two occupants of the divided Korean Peninsula.
- **Use of South Korean infrastructure**: Further research by SecurityScorecard threat hunters indicated that the actors likely used servers rented from South Korean IT service provider Daou Technology. North Korean actors often use compromised or illicitly obtained South Korean infrastructure, either in the hopes of blending in with their South Korean targets or to avoid revealing themselves as North Koreans by using infrastructure from a neighboring country that speaks the same language.

Timeline

- **December 5, 2023**: South Korean authorities reported that the North Korea-linked threat actor group tracked as Andariel had stolen over 1.2 TB of data from defense contractors and other South Korean organizations.
- **Methodology:** The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team consulted publicly available information, SecurityScorecard's internal datasets, and a strategic partner's network flow (NetFlow) data to develop further insights into the activity discussed in these reports.

Key findings

The STRIKE Team's comprehensive analysis revealed new details:

- **Hanwha Corporation targeted**: Hanwha Corporation, a prominent South Korean conglomerate, appears to be one of the targets of the reported attacks. The company's involvement in anti-drone air defense laser weaponry further confirms its significance as a target.
- **Indicators of Compromise (IoCs) and TTPs**: While the December reports lacked specific IoCs and TTPs, a report by South Korean cybersecurity company AhnLab provided valuable information on recent, though not necessarily linked, Andariel activity, revealing the use of multiple malware strains, including TigerRAT, NukeSped, BlackRAT, and LilithRAT, associated with Andariel.
- **Daou Technology involvement**: The attackers employed servers linked to South Korean IT service provider Daou Technology, reflecting their reliance on local infrastructure.
- **Potential compromise indications**: Suspicious email communications originating from an @hanwha[.]com email address suggests a potential compromise of Hanwha's resources. This could be related to phishing or spam distribution, possibly indicating unauthorized access, though this access may not be APT-related.

Background

On December 5, South Korean authorities reported that the threat actor group tracked as Andariel, which analysts assess to be a unit of the Reconnaissance General Bureau of the Army of Democratic People's Republic of Korea (DPRK), had stolen over 1.2 TB of data from South Korean defense contractors, other critical infrastructure organizations, and major South Korean businesses.

While the public reports do not specifically name the affected organizations, one may imply that Hanwha Corporation was among the defense contractors targeted; it notes that one of the targets had worked on anti-drone air defense laser weaponry. Hanwha won a contract to produce technology fitting that description in May 2021.

Although the December 5 reports do not identify specific indicators of compromise (IoCs) or tactics, techniques, or procedures (TTPs) linked to the threat activity they discuss, they note that it used servers rented from an unspecified South Korean company.

South Korean cybersecurity company AhnLab published a report that does, however, contain IoCs and TTPs associated with recent Andariel-attributed activity (and other threat activity linked to the North Korean government) on November 10. That report highlights the use of four different strains of malware: TigerRAT, NukeSped, BlackRAT, and LilithRAT.

The STRIKE Team consulted publicly available information, SecurityScorecard's internal datasets, and a strategic partner's network flow (NetFlow) data to develop further insights into the activity discussed in the December 5 reports. This yielded findings that may indicate that Hanwha suffered a compromise. It additionally offered information suggesting that South Korean IT service provider Daou Technology is the company that provided the rented servers mentioned in the public reports.

One file submitted to cybersecurity information-sharing platform VirusTotal on November 7 may suggest that Hanwha suffered a compromise; it contains one email message forwarding another, originating from an @hanwha[.]com email address. However, the party forwarding the original message (the one containing Hanwha's domain) asks, "스팸 맞겠죠?" ("It's spam, right?").

A recipient treating a message from a Hanwha account as spam may suggest abuse of Hanwha email accounts, which could indicate a compromise if the files do indeed reflect the use of Hanwha email accounts for phishing or the distribution of spam. Given that Hanwha itself would be unlikely to be responsible for such activity, it could instead reflect an unauthorized party's access to Hanwha resources. However, such access may not be related to the breaches attributed to Andariel, given that other threat actors have targeted Hanwha in the recent past. For example, the LockBit ransomware group claimed responsibility for an attack against Hanwha in September 2023.

STRIKE Team researchers identified and investigated recent IoCs linked to Andariel and other North Korean threat actor groups to develop further insights into the activity discussed in the recent reports. All of the IP addresses that researchers identified or which appeared in recent lists of Andariel-linked IoCs belong to two service providers, one of which (the Daou mentioned above Technology) is South Korean.

The November AhnLab report reported that the following IP addresses had carried out command and control (C2) communications with Andariel-linked malware or served downloads of it:

- 27.102.115[.]207
- 27.102.118[.]204
- 84.38.132[.]67
- 109.248.150[.]147
- 185.29.8[.]108
- 27.102.128[.]152

Of the above IP addresses, three, 27.102.115[.]207, 27.102.118[.]204, 27.102.128[.]15, belong to South Korean IT service provider Daou Technology, and three, 84.38.132[.]67, 109.248.150[.]147, and 185.29.8[.]108, belong to European service provider DataClub S.A.

STRIKE Team researchers identified an additional group of IP addresses belonging to these same providers when investigating other recently-circulated malware samples linked to DPRK-backed threat actor groups.

Daou Technology:

- 27.102.134[.]33
- 27.102.70[.]192
- 27.102.114[.]79
- 27.102.113[.]88
- 27.102.107[.]234
- 27.102.107[.]233
- 27.102.107[.]235
- 27.102.107[.]224
- 27.102.127[.]240
- 27.102.107[.]230

DataClub S.A.

- 109.248.150[.]13
- 109.248.150[.]179

A file that the vendors who contribute detections to VirusTotal have linked to two malware families named in the November AhnLab report (TigerRAT and NukeSped), which first appeared in VirusTotal on December 9, 2022, communicates with two of the above Daou Technology IP addresses, 27.102.134[.]33 and 27.102.70[.]192.

A sample of the TinyNuke malware, which vendors have linked to another DPRK-based threat actor group, Kimsuky, first appeared on VirusTotal on October 24, 2021, but appeared most recently on June 15, 2023. It communicates with 27.102.114[.]79.

A previous NukeSped sample, which first appeared in VirusTotal on August 27, 2023, and then appeared in an August 31 AhnLab report about Andariel, contains (and communicates with) 27.102.113[.]88 (one of the Daou Technology IP addresses above). A more recent sample with the same Rich PE header hash, 92baf2d405053814d84d8dfbd1001102, subsequently appeared on VirusTotal on September 5. That file features a different embedded Daou Technology IP address, 27.102.107[.]234.

27.102.107[.]234 has also been observed serving downloads of another file vendor's link to Andariel, first submitted to VirusTotal on September 7, 2022, but last analyzed on November 27, 2023. Two other Daou Technology IP addresses, 27.102.107[.]233 and 27.102.107[.]235, have also served downloads of it, and it contacts another Daou Technology IP address, 27.102.107[.]224.

An IP address contacted by the previous sample, 27.102.107[.]235, is also one that a file identified in a February report on Andariel activity contacts, as is an additional Daou Technology IP address, 27.102.107[.]230.

Three files most recently submitted to VirusTotal in Summer 2023 but created in Spring 2021, all of which vendors have linked to the Kimsuky threat actor group, communicate with the same Daou Technology IP address, 27.102.127[.]240, which analysts previously linked to Kimsuky activity in October 2021.

Given the above links between its IP addresses and activity attributed to North Korean threat actor groups, including Andariel, Daou Technology may be the domestic provider discussed (but not named) in the December 5 reports.

To develop further insights into the IP addresses linked to recent Andariel activity and North Korean cyber activity more generally, STRIKE Team researchers collected two traffic samples using a strategic partner’s network flow (NetFlow) data. The first of these focused on traffic involving the IP addresses named IoCs in AhnLab’s November report on Andariel activity. The second focused on traffic involving all IP addresses in North Korea’s four official IPv4 ranges. Then, bearing in mind that the use of virtual private networks (VPNs) often accompanies threat activity, researchers limited both samples to the results featuring IP addresses that SecurityScorecard’s partner has linked to VPNs and then compared these results to identify the VPN-linked IP addresses that appeared in both samples. This yielded the thirty-five IP addresses available in the appendix below. Those VPN-linked IP addresses communicating both with IP addresses named as IoCs in a recent report on Andariel activity and IP addresses located in North Korea may be more likely than others to represent assets used by Andariel or DPRK-linked threat actors.

Conclusion

Reporting on the recent Andariel incidents notes that South Korean police have seized the domestic servers believed to have been involved in them and begun verifying the identities of the provider's customers. Whether that includes the servers represented by the particular IP addresses above remains to be seen. Still, given the frequent use of Daou Technology IP addresses by Andariel and other DPRK-linked threat actor groups, it seems likely that Daou Technology is the provider involved. The European IP addresses identified above, all of which belong to DataClub S.A., may also merit further investigation, although jurisdictional issues may prevent their seizure by South Korean authorities.

This investigation should be considered trustworthy but preliminary. The STRIKE Team can, however, provide additional information, including further analysis of traffic contained in the present samples or by analyzing additional samples involving other Daou Technology or DataClub IP addresses, upon request.

Appendix: VPN IP addresses appearing in IoC and DPRK traffic samples

- 68[.]235[.]44[.]98
- 198[.]44[.]128[.]215
- 68[.]235[.]44[.]23
- 68[.]235[.]43[.]181
- 204[.]188[.]245[.]112
- 68[.]235[.]50[.]233
- 68[.]235[.]44[.]34
- 162[.]212[.]156[.]207
- 68[.]235[.]39[.]123
- 68[.]235[.]48[.]20
- 68[.]235[.]44[.]66
- 68[.]235[.]43[.]67
- 98[.]159[.]33[.]36
- 198[.]44[.]128[.]220
- 68[.]235[.]43[.]66
- 198[.]44[.]128[.]84
- 68[.]235[.]43[.]98
- 204[.]188[.]247[.]173
- 199[.]115[.]99[.]62
- 70[.]39[.]103[.]3
- 174[.]128[.]251[.]99
- 198[.]54[.]128[.]115
- 161[.]129[.]143[.]1
- 104[.]248[.]133[.]26
- 38[.]47[.]179[.]3
- 38[.]47[.]179[.]12
- 38[.]47[.]179[.]11
- 103[.]178[.]153[.]233
- 38[.]47[.]179[.]13
- 161[.]129[.]142[.]215
- 104[.]245[.]131[.]162
- 38[.]47[.]179[.]14
- 204[.]188[.]232[.]195
- 38[.]47[.]179[.]10
- 121[.]200[.]63[.]162.

About SecurityScorecard

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard.com
info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

SecurityScorecard