North Korean Lazarus Group Now Working With Medusa Ransomware

By About the Author

Archived: 2026-04-05 19:12:18 UTC

North Korean state-backed attackers are now using the Medusa ransomware and are continuing to mount extortion attacks on the U.S. healthcare sector.

North Korea has long been involved in ransomware attacks and has been previously associated with the Maui and Play ransomware families. However, the Symantec and Carbon Black Threat Hunter Team has uncovered evidence North Korean actors using Medusa in an attack on a target in the Middle East. The same attackers also mounted an unsuccessful attack against a healthcare organization in the U.S.

Medusa, which is operated by the Spearwing cybercrime group, was launched in 2023 and is run as a ransomware-as-a-service, where affiliate attackers can deploy the ransomware in exchange for a percentage of ransom payments. More than 366 attacks have been claimed by attackers using Medusa.

Analysis of the Medusa leak site reveals attacks against four healthcare and non-profit organizations in the U.S. since the beginning of November 2025. Victims included a non-profit in the mental health sector and an educational facility for autistic children. It is unknown if all these victims were targeted by North Korean operatives or if other Medusa affiliates were responsible for some of these attacks. The average ransom demand in that period was $260,000.

History of extortion

One of the prime movers in mounting North Korean ransomware attacks in recent years has been the Lazarus sub-group Stonefly (aka Andariel). For many years, Stonefly was thought to be solely engaged in espionage attacks, particularly against high-value targets. However, the group became involved in ransomware attacks approximately five years ago. Its involvement in digital extortion came to public attention in July 2025, when the U.S. Justice Department indicted a North Korean man named Rim Jong Hyok on charges related to a ransomware campaign against U.S. hospitals and other healthcare providers. Rim is alleged to be a member of Stonefly, which is linked to the North Korean military intelligence agency, the Reconnaissance General Bureau (RGB).

The indictment shed some light on the motivation behind Stonefly's move into ransomware. It alleged that the group was using the proceeds of ransomware attacks to fund its espionage activities, including attacks against the defense, technology, and government sectors in the U.S., Taiwan and South Korea.

The indictment, and a $10 million reward for information on Rim, did not appear to deter Stonefly from mounting further attacks. In October 2024, our Threat Hunter Team found evidence of intrusions against three different U.S. organizations. Although no ransomware was successfully deployed, the attacks appeared to be financially motived since all victims were private companies and involved in businesses with no obvious intelligence value.

In the same month, Palo Alto Unit 42 reported that it had begun collaborating with the Play ransomware group.

Attacker toolset

Lazarus is using a range of tools in its current ransomware campaigns. These include:

- Comebacker: A custom backdoor and loader exclusively associated with Lazarus.
- Blindingcan: A remote access Trojan (RAT) associated with Lazarus.
- ChromeStealer: A tool for extracting stored passwords from the Chrome browser.
- Curl: An open-source command-line tool for transferring data using various network protocols.
- Infohook: Information-stealing malware.
- Mimikatz: A publicly available credential dumping tool.
- RP_Proxy: A custom proxying tool.

Attribution

While the current Medusa ransomware attacks are undoubtedly the work of Lazarus, the blanket designation for North Korean state-sponsored activity, it is unclear which Lazarus sub-group is behind them. While the TTPs – extortion attacks against the U.S. healthcare sector – are like previous Stonefly attacks, the malware tools used are not exclusive to Stonefly. For example, the Comebacker backdoor has previously been reported to be associated with the Pompilus group (aka Diamond Sleet).

Few scruples

The switch to Medusa demonstrates that North Korea's rapacious involvement in cybercrime continues unabated. North Korean actors appear to have few scruples about targeting organizations in the U.S. While some cybercrime outfits claim to steer clear of targeting healthcare organizations due to the reputational damage it may attract, Lazaurs doesn't seem to be in any way constrained.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

File indicators

15208030eda48b3786f7d85d756d2bd6596ef0f465d9c8509a8f02c53fad9a10 - Medusa ransomware

0842dd5c1f79f313ea08c49d1fb227654c32485b3f413e354dbe47b8a519a120 - Comebacker

202b03d788df6a9d22bbd2cbc01ba9c7b4a9caad0f78a4d420f8c2c30171a08d - Comebacker

61f3b09bcbae2fc2c98ccac7b2a0becdf5ddb28fe6a8b9c679fd574d58f8ca40 – Comebacker

8f6866532abd8400d244d0441be097f8209065ac43d9f864b2a6894f9da2880a – Comebacker

a12c84dabaffa868507807c645f7f0769ac848cc575a8c3b42dfb791aa5caeef – Comebacker

bf27c5e2591febe90e52cd99231526a342bc423000fe87cce44ef1c3acaeeab5 - Comebacker

60b942bbdac625300eeb11cccba5ed44f376634f73d3bc01a17e7a758c570a8e - Comebacker Loader

7a22880780c74b212e36ebb871af4af26a620326c456cf96a3dfb1481ee436cc – Loader

ab3e3a8673ba5da40b325b160a782cf2f03547d9b489e87d9546da35a65d62d6 – SSH Loader

16d57ff889aab5b8c8a646da99d5a9335177fb4c158191baa1cf199f0e818d3a - File used for DLL sideloading

3e3e0519a154266da1558e324c9097e7c39ccf88f323f2f932f204871d1b91cb - RP_Proxy

60aaf6c01ba0c15b78902fd4be12c7e5f2323ade8f9db7e9fbbb9ec0c2afc8ba - RP_Proxy

7530323c3976687a329e06bb7b7f95017f2cfd408f6a5261cb2f0c6b6f18f081 - RP_Proxy

ce4fcb97ada09a42c03c3456c5fe09d805948a95efaf365eb1cd2b4e82013990 - RP_Proxy

db98d087d4cdb2a82096df424f86edea8d4730543a2005f43bede9ffc6123791 – Mimikatz

e24e4c949894b08a66b925b6c55f12d1b3c69adc95b79e99a31315e289d193fc - ChromeStealer

61c49c8f116cb7118dee613536085cfaa7a59d5f49c36b9ff432be7b8a7f25f0 – Credential Stealer

18049366331a5f0afd54c2ca84e6ed302e81d58a162673715fee865541d53b11 - Suspicious file

313ce75f0f47e2a8fd66120fcbcaa6226fc0c4862b585b8e04850153f97bc4a3 - Suspicious file

3b8850bad0cb3ebae477b3787844b892bb0e4f7bd9c9e8b507898a726e7e2763 - Suspicious file

416545b9e844d3d924e162951a8ee885f3885e054a196ccdc659fd9d1f1911a6 - Suspicious file

4a702c784eb997a170bea81778a770a86e61c759ff95ca0ad958ceca55c20c7b - Suspicious file

52293b53ca5209bc49f009288cf6fc80c9f787c9c735cc06e7dc6fc9fcdaf61d - Suspicious file

55cb4a851372237a5ba4bf187e37b0d599f3ffa13ac17464130744614353bd07 - Suspicious file

63432828de42e43ea3715157da5439c40e5c371eefd7c1892b25f396c1018cc8 - Suspicious file

6428ef885c54b8154bd86a5d849fb8cc8c04f39e72188117119b9e2832b99ee6 - Suspicious file

6ad1a57ce20b422b77bab84a8daebf4e7262543742b2fdcbcacde3f7780d9046 - Suspicious file

6ba46c392bdc330ceef2aeb984c63c89d673a090dd68d3258e4aa7e20e5c098d - Suspicious file

84168ee4e290690985358dfc497b98a22ef279a01179b93ff4e6c9c5e1ee26e4 - Suspicious file

918e2a5a01fdb0ad462b0242e4f23d51111031052a1ebd6a32d22be9cbd8dfb8 - Suspicious file

932b9ec79c782f06b3c8d267af916df41328ddb8235d021ea7f945dc4082d991 - Suspicious file

9cb10407ca3c9e8c1a069ebb4c677d8889117c1bc5206fbf16f47ebb13ef34b9 - Suspicious file

a670d8818a6efe2919c18c740ef4f3478551b28481d0a1591539be45ceca2171 - Suspicious file

a957b5dd5f555be8431df3f35b707c149b83436d19cc3f8bbd867317a6f624b1 - Suspicious file

b42345567556a01d34daf262f95fdeb02f259271afbea93fb684b9656d14e568 - Suspicious file

b8a9533a21127ff5005352d41581c5631598704e220120b623fad16e3ec2ae51 - Suspicious file

bf05b1ace61aeebd251940b40624fe22a345300fc6a53a472357f9586e8e4e57 - Suspicious file

c69acc7364da828f098394b1a6907788d4fd379ed2af7d966e86a2becea4c0ad - Suspicious file

cf5e38d65bef38654080635fcb76890e3e0548626b0598bc8090b18116220389 - Suspicious file

cfe33c6faacc824fcb475d450d6ba19316884fad4c85f563a330a86d03ecff0c - Suspicious file

d80daa7b30732b2b71d63a5881a254d12eb0d499a015dc4c98602caa2001d2a3 - Suspicious file

df1b9ec31fa4578dee7668207064de7185798801bb032c715aa24cce7e35bcda - Suspicious file

f0f4423cd8d5ceafb4e4a18014ff4ed8913021d83bc2c3a973a419b9fe466c19 - Suspicious file

fdd4b78aa4e0914f3bcdc2632338ebbd300fdc3f05a3df85a5a3067f97627e45 - Suspicious file

35a11a68b0ce862bdc7450735237e56cf70156870b0527ec624f0a57076c09c7 - Suspicious file

a55bc262c5218c6bdaebcf4618154312ff0540b00c382ab34e805699ce3fcc31 - Suspicious file

bedada1c52e9bcceff8c6b542d74518afcce66f955ac6f1ab58aa43b3865fe9f - Suspicious file

Network indicators

23.27.140[.]49

23.27.140[.]135

23.27.140[.]228

23.27.124[.]228

amazonfiso[.]com

human-check[.]com

illycoffee[.]my

illycafe[.]my

markethubuk[.]com

sictradingc[.]com

trustpdfs[.]com

zypras[.]com
