Severity

High

Analysis Summary

Stonefly — aka DarkSeoul, BlackMine, Operation Troy, and Silent Chollima, is a cyberespionage group that originally made headlines in July 2009, when it launched DDoS attacks on a variety of South Korean, government, and financial websites. However, in recent years, they have reduced their attention to exclusively espionage operations against high-value targets.

Stonefly's operations appear to be part of a larger North Korean-sponsored campaign to obtain information and intellectual property, with another North Korean group, Pompilus, conducting a bigger trawl across numerous sectors. A most recent attack discovered by security researchers was against an engineering firm that works in the energy and military sectors. The attackers breached the organization most likely by exploiting the Log4j vulnerability (CVE-2021-44228) on a public-facing server. The attackers then compromised 18 other computers.

Stonefly's tools and techniques are still evolving and due to its capabilities and emphasis on gathering sensitive data, the group is one of the most potent North Korean cyber threat actors active today.

Impact

- Information theft and espionage
- Exposure of sensitive data

Indicators of Compromise

Domain Name

- tecnojournals[.]com
- semiconductboard[.]com
- cyancow[.]com
- bluedragon[.]com

MD5

- 9dcc3e4dafc47d6f505880d7eb43fa93
- a4cddfaa5a1fc2abf8a920bee84ce8e3
- c99dde8c7d68c1776aaf52275a6d9cd2
- 8df48fa69cb7b4c99939702caa70d1a9
- 47e001253af2003985f15282cdc90a1c

SHA-256

- 9ca9f414b689fc903afb31401615581488596 6b0e30b21b642819d53ba94533c
- 28d0e945f0648bed7b7b2a2139f2b9bf1901feec39ff4f6c0315fa58e054f44e
- b4a85ef01b5d8058cf94f3e96c48d86ce89b20295e8d1125dc3fc1c799a75789
- de00c0111a561e88d62fd84f425a6febc72e01e2e927fb76d01603319a34b4b3
- 14f0c4ce32821a7d25ea5e016ea26067d6615e3336c3baa854ea37a290a462a8

SHA-1

- b9fe3c1d3d5dbf330efc81c4dd5ec4ef405bc412
- 0365fe05e2de0f327dfaa8cd0d988dbb7b379612
- 817c2f378bacdae18b3d71b3b76a02109975e2e5
- 78c9fe7590df8252e01ccfc4dccc79c30d580994
- 6ee6664df9bfb47d97090492b6cde68bf056a42a

URL

- https[:]//tecnojournals[.]com/review
- https[:]//tecnojournals[.]com/general
- https[:]//semiconductboard[.]com/xcror
- http[:]//cyancow[.]com/find
- https[:]//bluedragon[.]com/login

Remediation

- Exercise caution when receiving messages from unknown senders.
- Block all threat indicators at your respective controls.
- Keep your software updated to the latest patches.
- Search for IOCs in your environment.