Severity

High

Analysis Summary

Lazarus APT (aka AppleWorm, APT C-26, Group-77, Guardians of Peace, Hidden Cobra, Official 91, Red Dot, Term.Hermit, or Zinc) is one of North Korea's most sophisticated threat actors, operating since at least 2009. Initially, they concentrated on South Korea. It has recently shifted its focus to worldwide targets and began initiating assaults for monetary gain. This actor has been linked to attacks in South Korea, the United States, Japan, and a number of other nations. Lazarus APT is suspected of being behind a number of diverse efforts, including cyberespionage, attacks on financial institutions, government agencies, and the military.

This group is said to be behind the wiper attack on Sony Pictures Entertainment in November 2014 as part of Novetta's Operation Blockbuster campaign. Lazarus Group's malware is linked to other known campaigns such as Operation Flame, Operation Troy, DarkSeoul, Operation 1Mission, and Ten Days of Rain

Recently Lazarus has been linked by the U.S Government to the $625 Million Ronin Network Heist.

"There has been a security breach on the Ronin Network. Earlier today, we discovered that on March 23rd, Sky Mavis's Ronin validator nodes and Axie DAO validator nodes were compromised resulting in 173,600 Ethereum and 25.5M USDC drained from the Ronin bridge in two transactions (1 and 2)." reads a statement published by the company. "The attacker used hacked private keys in order to forge fake withdrawals. We discovered the attack this morning after a report from a user being unable to withdraw 5k ETH from the bridge."

Impact

- Information Theft and Espionage
- Exposure of Sensitive Data

Indicators of Compromise

Domain Name

- happy[.]nanoace[.]co[.]kr
- mariamchurch[.]com

IP

- 52[.]79[.]118[.]195
- 61[.]81[.]50[.]174

MD5

- b3a8c88297daecdb9b0ac54a3c107797

SHA-256

- a881c9f40c1a5be3919cafb2ebe2bb5b19e29f0f7b28186ee1f4b554d692e776

SHA-1

- 46660f562fe01b5df0e1ac03dd44b4cc8d2fa5f5

URL

- http[:]//happy[.]nanoace[.]co[.]kr/Content/rating/themes/krajee-fas/FrmAMEISMngWeb[.]asp
- https[:]//mariamchurch[.]com/board/news/index[.]asp

- https[:]//www[.]aumentarelevisite[.]com/img/context/offline[.]php

Remediation

- Always be suspicious about emails sent by unknown senders.
- Never click on links/attachments sent by unknown senders.
- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.