Severity

High

Analysis Summary

Lazarus APT 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.

Impact

- Information Theft and Espionage
- Exposure of Sensitive Data

Indicators of Compromise

Domain Name

- cloud[.]beenos[.]biz
- it[.]zvc[.]capital
- venturelabo[.]co
- azureword[.]com

URL

- https[:]//cloud[.]beenos[.]biz/_D5l8MJUYh2/xtxjq441tQ/KxQAWNWRdM/lr1bYSy+/nh6rr4cuaj/eK9Ww==
- https[:]//cloud[.]beenos[.]biz/gM7Sy9dz+/tqs+Aikg/fK_i2afRzg/Ac0r_r1bYS/y+nh6rr4/cuajeK9Ww==
- https[:]//cloud[.]beenos[.]biz/NbmU3+Ad+nKc4nYo1/VN1mMyIelT/5y_yqr1bYS/y+nh6rr4/cuajeK9Ww==
- https[:]//cloud[.]beenos[.]biz/BJD4k8WFV_K/xtxjq441tQ/KxQAWNWRdM/lr1bYSy+/nh6rr4cuaj/eK9Ww==
- https[:]//cloud[.]beenos[.]biz/NZLCuY57xpP/zqCbWksZKm/+9aCZ8vZ/bLOr1bYSy+nh6rr4cu/ajeK9Ww=/=
- https[:]//doc[.]venturelabo[.]co/bC+ZPs40y/VgIBvJEDoX/3VADqXGLEF/sP9B4PYHt6/KN5Y=
- https[:]//it[.]zvc[.]capital/C5MplvLKOqh/msUsLMGlyq/vAzw+xIt/kCYVUO1eI4/Lb9k=

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.