Lazarus

download.png
Image not found or type unknown

Introduction

Lazarus, also known as Hidden Cobra or Zinc, is a **North Korean state-sponsored hacking group** that has been active since 2009. The group is one of the world's most active threat actors and has been behind large-scale cyber-espionage and ransomware campaigns. Lazarus has often switched targets through time, probably according to nation-state interests.

Lazarus is responsible for infamous cyber incidents such as the attack on Sony Pictures in 2014 and the spread of the WannaCry ransomware in 2017 . The group has also been spotted attacking the defense industry and cryptocurrency markets. Lazarus is known for its involvement in several high-profile bank heists. The group has also targeted energy providers in the U.S., Canada, and Japan with a new malware arsenal .

Also Known As

"Operation DarkSeoul", "Dark Seoul", "Hidden Cobra", "Hastati Group", "Andariel", "Unit 121", "Bureau 121", "NewRomanic Cyber Army Team", "Bluenoroff", "Subgroup: Bluenoroff", "Group 77", "Labyrinth Chollima", "Operation Troy", "Operation GhostSecret", "Operation AppleJeus", "APT38", "APT 38", "Stardust Chollima", "Whois Hacking Team", "Zinc", "Appleworm", "Nickel Academy", "APT-C-26", "NICKEL GLADSTONE", "COVELLITE", "ATK3", "G0032", "ATK117", "G0082"

Region Focus

1. South Korea
2. Bangladesh Bank
3. Sony Pictures Entertainment
4. United States
5. Thailand

6. France
7. China
8. Hong Kong
9. United Kingdom
10. Guatemala
11. Canada
12. Bangladesh
13. Japan
14. India
15. Germany
16. Brazil
17. Thailand
18. Australia
19. Cryptocurrency exchanges in South Korea

Technology

Lazarus has used a variety of techniques to carry out its attacks. The group has been involved in large-scale cyberespionage campaigns, ransomware campaigns, and even attacks against the cryptocurrency market. Lazarus has also been observed using the MATA malware framework to target various industries for cybercrime purposes, such as stealing customer databases and spreading ransomware .

Techniques

The disruptive operations performed by Lazarus involve DDOS attacks and Wipers with time-based triggers. These include KILLMBR with a hard-coded wiping date, and QDDOS, which has duration date that wipes data ten days after infection. DESTOVER, a backdoor equipped with wiping capabilities, is another .

CVEs Focus

- CVE-2021-21551: A vulnerability in a Dell driver that allows user-mode applications to read and write kernel memory. The Lazarus Group used this vulnerability to bypass security solutions and execute malicious code2
- CVE-2017-0199: A vulnerability in Microsoft Office that allows remote code execution via specially crafted files. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails.

- CVE-2017-11882: A vulnerability in Microsoft Office that allows arbitrary code execution via a maliciously modified equation editor. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails.
- CVE-2018-4878: A vulnerability in Adobe Flash Player that allows remote code execution via a specially crafted SWF file. The Lazarus Group used this vulnerability to deliver malware to their targets via phishing emails or compromised websites.

Industry Attacked

Lazarus has attacked various industries such as automotive, academic, defense sectors in Eastern Europe and other parts of the world . The group has also targeted financial institutions and energy providers in the U.S., Canada, and Japan.

Reference

1. https://github.com/MISP/misp-galaxy/blob/main/clusters/threat-actor.json

---

Revision #3
Created 24 October 2023 12:57:09 by Admin
Updated 24 October 2023 14:19:35 by Admin