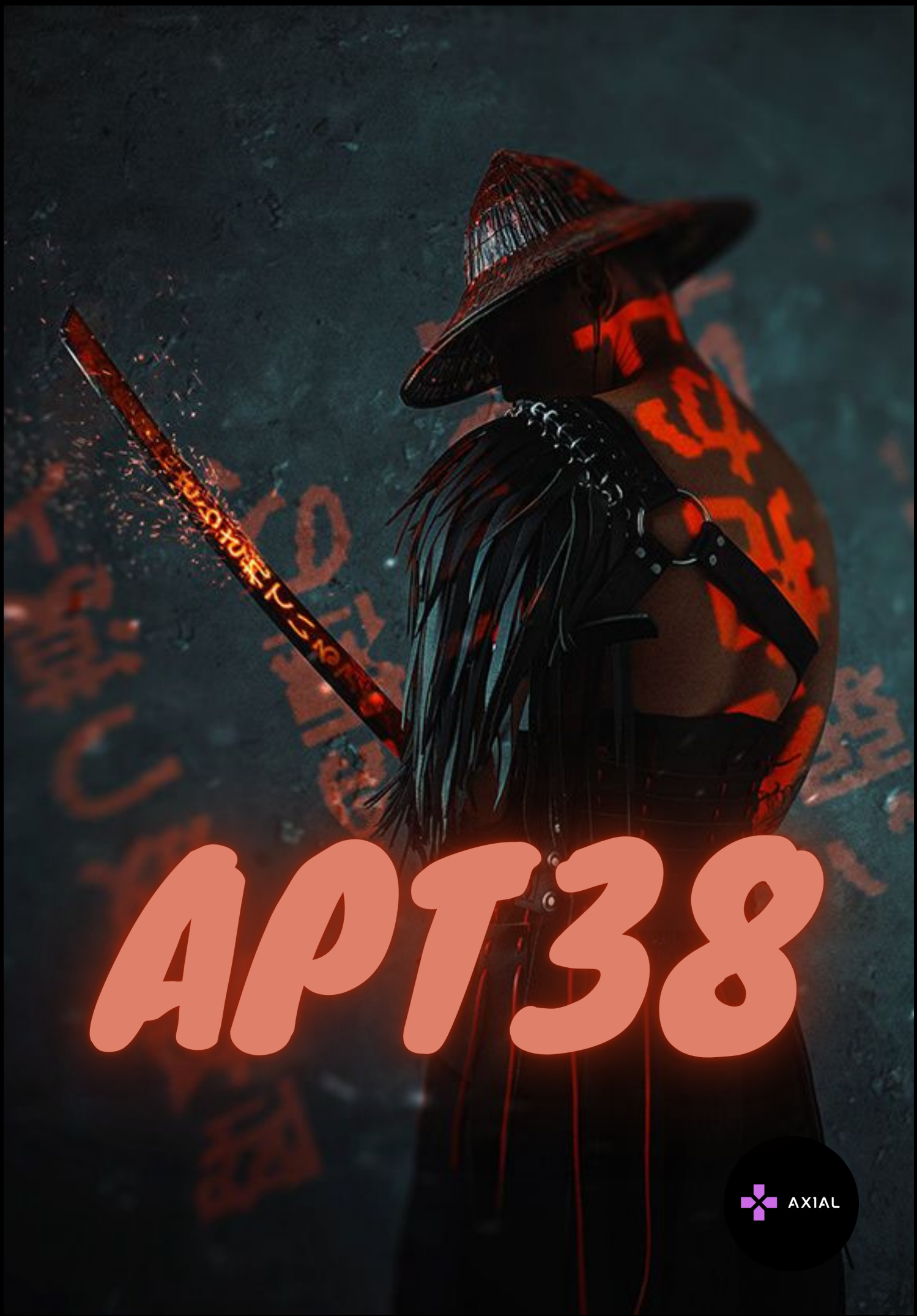
APT38
AXIAL

A SURVEY ON APT38: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

APT38 a.k.a. Stardust Chollima, Bluenoroff, or ATK 117 is a subgroup of Lazarus Threat Group that originates from North Korea. They were first seen in 2014 and their operation focuses on Financial Crime. Primarily focused on currency generation, APT38 launched attacks against financial institutions in Latin America, Asia, and Africa. These intrusions are monetized by fraudulent SWIFT transfers and ATM cashouts. They have been active since 2014.

II. TARGET SECTORS

APT38 primarily targets its victims with the aim of acquiring funds. According to CrowdStrike they have not directly observed APT38 conduct intelligence-gathering or destructive operations.

III. IOC

MD5

- d08f1211fe0138134e822e31a47ec5d4
- b27881f59c8d8cc529fa80a58709db36
- 3c9e71400b72cc0213c9c3e4ab4df9df
- 0edbad9e6041d43f97c7369439a40138
- 97aaf130cfa251e5207ea74b2558293d
- 62217af0299d6e241778adb849fd2823
- 0dd7da89b7d1fe97e669f8b4156067c8
- 61075faba222f97d3367866793f0907b
- 1205c4bd5d02782cc4e66dfa3fef749c
- 92d618db54690c6ae193f07a31d92098
- 3e6be312a28b2633c8849d3e95e487b5
- 41a6d7c944bd84329bd31bb07f83150a
- 7343f81a0e42ebf283415da7b3da253f
- 73471f41319468ab207b8d5b33b0b4be
- 84a3f8941bb4bf15ba28090f8bc0faec
- b04fabf3a7a710aafe5bc2d899c0fc2b

IV. METHODS USED

This actor uses techniques such as code protection tools like Enigma protector, password protected executables and secure deletion functions to remain hidden on target system for long periods of time by avoiding legacy security products.

V. LINKS TO OTHER THREAT GROUPS

Stardust Chollima is a splintered off portion of the Lazarus Group with the objective of stealing money to fund itself.

AX1AL

VI. ENGAGEMENTS

- **2015**
  - Duuzer Backdoor targets South Korean Manufacturing Industry.
  - Symantec found evidence of a bank in Philippines had been attacked by APT38 using malware: Backdoor.Fimlis, Backdoor.Fimlis.B, Backdoor.Contopee.
  - A Vietnamese bank foiled a plot to transfer large sums of money using SWIFT messaging system. It was noted that the malware appeared to be tied to the Lazarus Group.
- **2016**
  - SWIFT Attack on Banco del Austro in Ecuador
  - Watering Hole attacks used to target organizations in 31 countries.
- **2017**
  - Securelist uncovered APT38's campaign which had them sending spear-phising emails containing an archived windows shortcut file. The infection chain started from this shortcut file is a complex multi-stage infection procedure.
  - SWIFT Attack on Far Eastern International Bank (FEIB) in Taiwan moving funds from its accounts to multiple overseas beneficiaries.
- **2018**
  - Mexico's Bank Bancomext had foiled APT38's bank heist
  - Chile's largest financial institution was hit with a Wipe Malware, which reportedly destroyed 9,000 workstations and 500 servers, was actually cover for a larger plot to compromise endpoints handling transactions on the SWIFT network. Investigators said $10 million was stolen from Banco de Chile and credited off to an account in Hong Kong.
  - APT38 is believed responsible for stealing $13.5 million from India's Cosmos Bank.
  - ATM breach of Redbanc in Chile utilized PowerRatankba, a malware strain previously linked to Lazarus Group hacks

VII. ATTRIBUTIONS

- FireEye noted that there are many similarities between APT38 and attacks launched by other North Korean linked groups, including Lazarus and the activity it tracks as TEMP.Hermit indicating that the activity is made up of multiple operational groups primarily linked together with shared malware development resources and North Korean state sponsorship. APT38's attacks are exclusively cyber heists whose likely goal is to raise money for the regime.

VIII. REFERENCES

- https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-april-stardust-chollima/
- https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
- https://securelist.com/apt-trends-report-q2-2020/97937/
- https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html
- https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret
- https://threatpost.com/lazarus-apt-spinoff-linked-to-banking-hacks/124746/