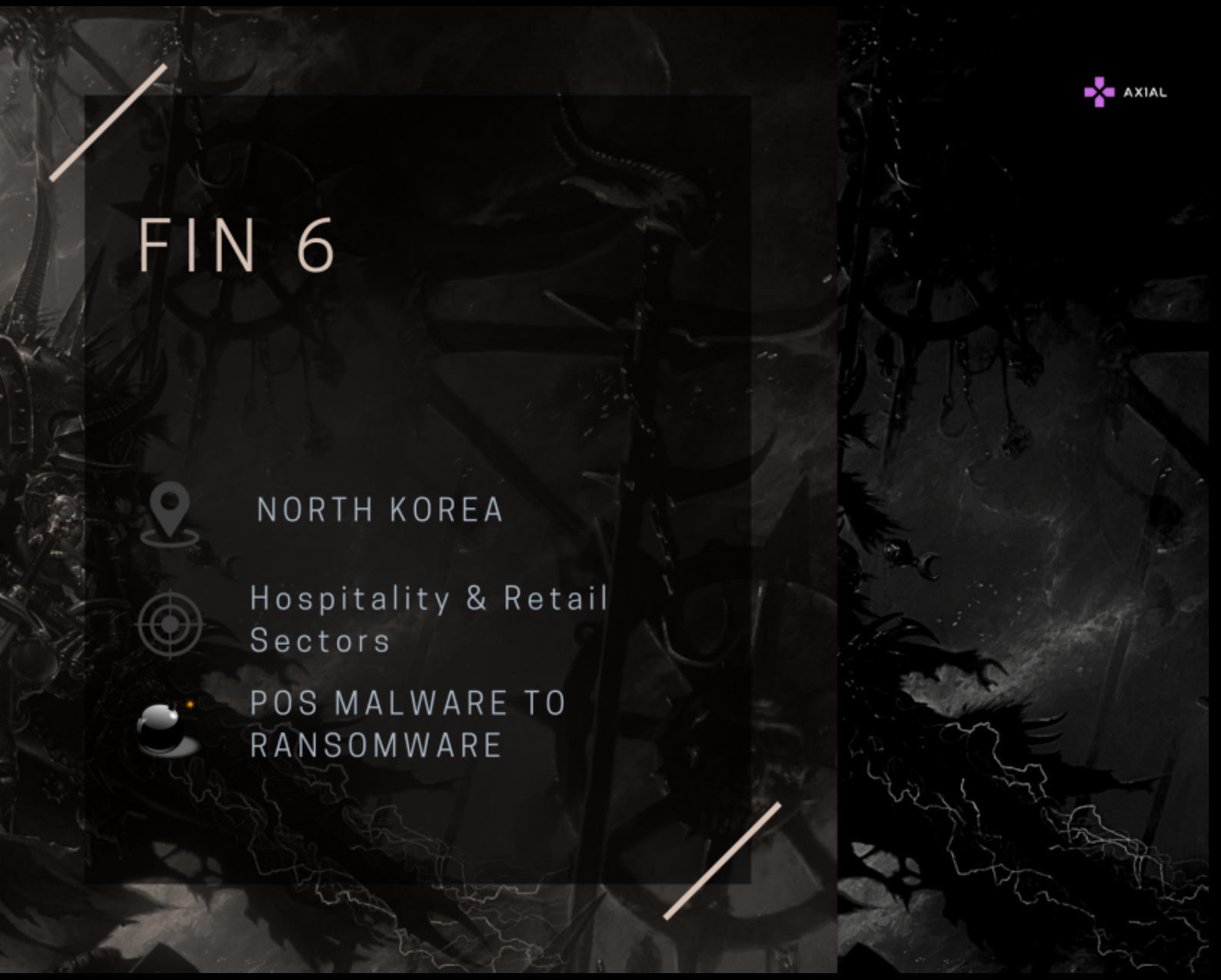
FIN 6



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON FIN 6 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

FIN 6 is a threat group which is attributed to be based out of North Korea , focuses on financial gain.

II. TARGETS

The targets of this threat group has been focused on Chemical, Energy, Hospitality, Manufacturing, Retail.

III. METHODS USED

This group has been using PowerShell to execute an encoded command, they also leveraged Windows services to execute powershell commands.They have been deploying Ryuk or Lockergoga ransomware , also later for later movement they used encoded powershell commands to install Cobalt Strike on compromised systems.

IV. CAMPAIGNS

This group has been involved in sophisticated attacks on POS systems on 2019 around the globe. They have also infected the systems of Altran Technologies with malware, this group had also been involved with attacks on Norsk Hydro.

ATTRIBUTION

FIN6 is not a nation sponsored threat group , rather it is financially motivated but as it has been deploying Ryuk Ransomware onto it's campaigns and Ryuk is linked to the North Korean threat group APT-38 attributed by Fireeye.

V. IOCS

Hashes , Network & IPs

031dd207c8276bcc5b41825f0a3e31b0
0f9931210bde86753d0f4a9abc5611fd
12597de0e709e44442418e89721b9140
32ea267296c8694c0b5f5baeacf34b0e
395d52f738eb75852fe501df13231c8d
39b7c130f1a02665fd72d65f4f9cb634
3c5575ce80e0847360cd2306c64b51a0
46d781620afc536afa25381504059612
4ec86a35f6982e6545b771376a6f65bb
73e7ddd6b49cdaa982ea8cb578f3af15
8452d52034d3b2cb612dbc59ed609163
8c099a15a19b6e5b29a3794abf8a5878
9d3fdb1e370c0ee6315b4625ecf2ac55
d2f9335a305440d91702c803b6d046b6
34187a34d0a3c5d63016c26346371b54

31.220.45[.]151
46.166.173[.]109
62.210.136[.]65
89.105.194[.]236
93.115.26[.]171
103.73.65[.]116
176.126.85[.]207
185.202.174[.]31
185.202.174[.]41
185.202.174[.]44
185.202.174[.]80
185.202.174[.]84
185.202.174[.]91
185.222.211[.]98

hxxps://176.126.85[.]207:443/7sJh
hxxps://176.126.85[.]207/ca
hxxps://pastebin[.]com/raw/0v6RiYEY
hxxps://pastebin[.]com/raw/YAm4QnE7
hxxps://pastebin[.]com/raw/p5U9siCD
hxxps://pastebin[.]com/raw/BKVLHWa0
hxxps://pastebin[.]com/raw/HPpvY00Q
hxxps://pastebin[.]com/raw/L4LQQfXE
hxxps://pastebin[.]com/raw/YAm4QnE7
hxxps://pastebin[.]com/raw/p5U9siCD
hxxps://pastebin[.]com/raw/tDAbbY52
hxxps://pastebin[.]com/raw/u9yYjTr7
hxxps://pastebin[.]com/raw/wrehJuGp
hxxps://pastebin[.]com/raw/tDAbbY52
hxxps://pastebin[.]com/raw/wrehJuGp
hxxps://pastebin[.]com/raw/Bber9jae

VI. REFRENCES

https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=FIN6%2C%20Skeleton%20Spider