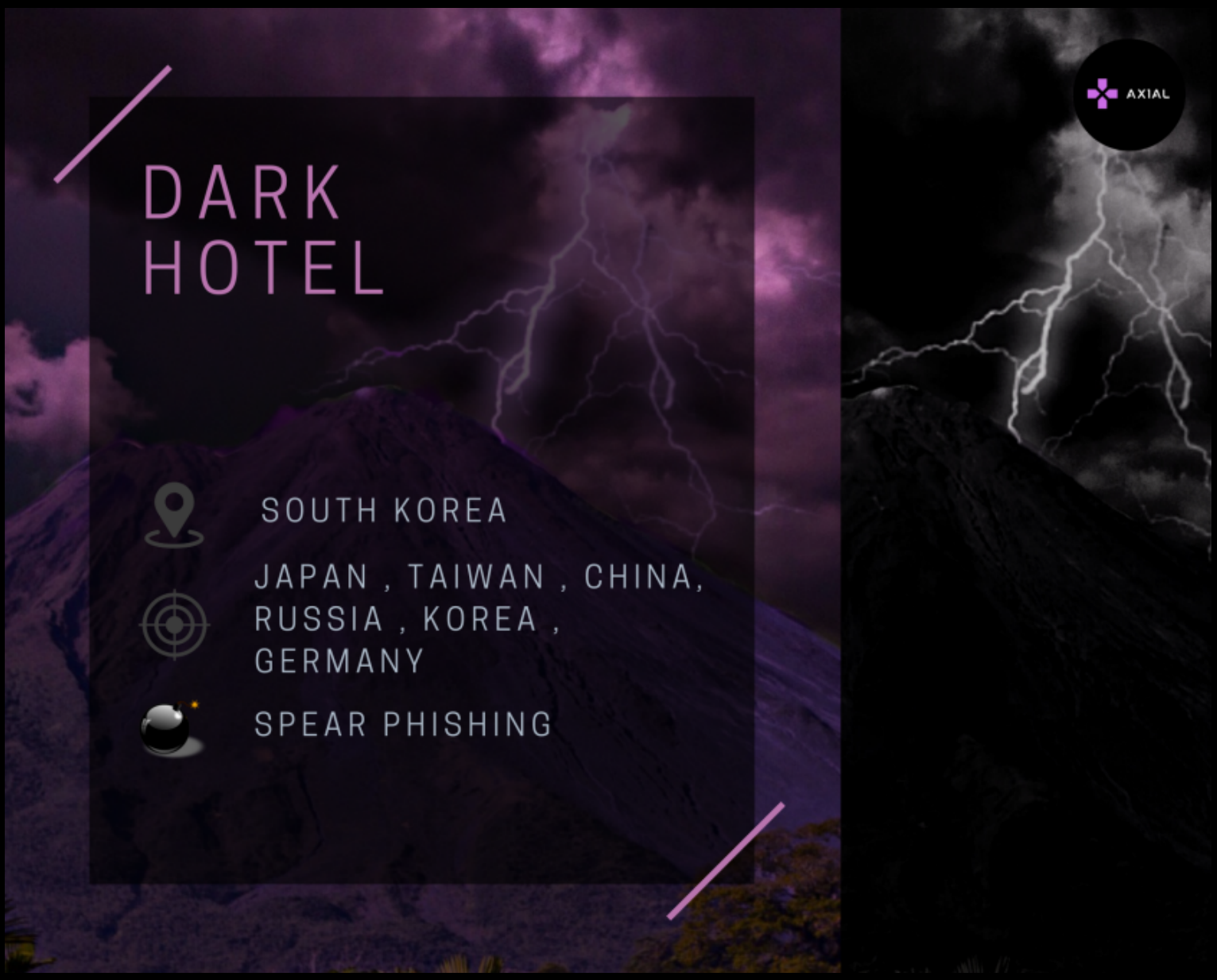
DARK HOTEL



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON DARK HOTEL ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Dark Hotel is a threat group based out of South Korea which also goes by various names like APT -C-06 and SIG25 .

II. TARGETS

Targets of this threat group are business travelers in the Asia-Pacific regiothey have been targeting military, energy , NGOs and various other critical sectors on various other multiple countries .

III. METHODS USED

This group uses zero-day exploits and CVE-2015-8651 & CVE-2018-8174

This group has also been using exploits leaked from Italian spyware maker Hacking Team .

This group has also been using spear phishing techniques .

IV. CAMPAIGNS

The campaigns of this group are as follows:

This group is linked to operation Dark Hotel .
This group has been linked to operation Daybreak.
This group is linked to operation Inexsmar .
This group has been linked to operation Powerfall. & The Gh0st Remains the Same.

ATTRIBUTION

The activities of the DarkHotel advanced persistent threat (APT) actor came to light in November 2014, when Kaspersky published a report detailing a sophisticated cyberespionage campaign targeting business travelers in the Asia-Pacific region. The group has been around for nearly a decade and some researchers believe its members are Korean speakers.

[cited from SecurityWeek]

AX1AL

V. IOCS

Hashes

df999d24bde96decdbb65287ca0986db98f73b4ed477e18c3ef100064bceba6d
c3a45aaf6ba9f2a53d26a96406b6c34a56f364abe1dd54d55461b9cc5b9d9a04
c613487a5fc65b3b4ca855980e33dd327b3f37a61ce0809518ba98b454ebf68b
1074654a3f3df73f6e0fd0ad81597c662b75c273c92dc75c5a6bea81f093ef81
dcd2531aa89a99f009a740eab43d2aa2b8c1ed7c8d7e755405039f3a235e23a6
c0a0266f6df7f1235aeb4aad554e505320560967248c9c5cce7409fc77b56bd5

C2
sixindent[.]epizy[.]com
goodhk[.]azurewebsites[.]net
tzeplin[.]atwebpages[.]com
www.comcleanner[.]info

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=DarkHotel
https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/