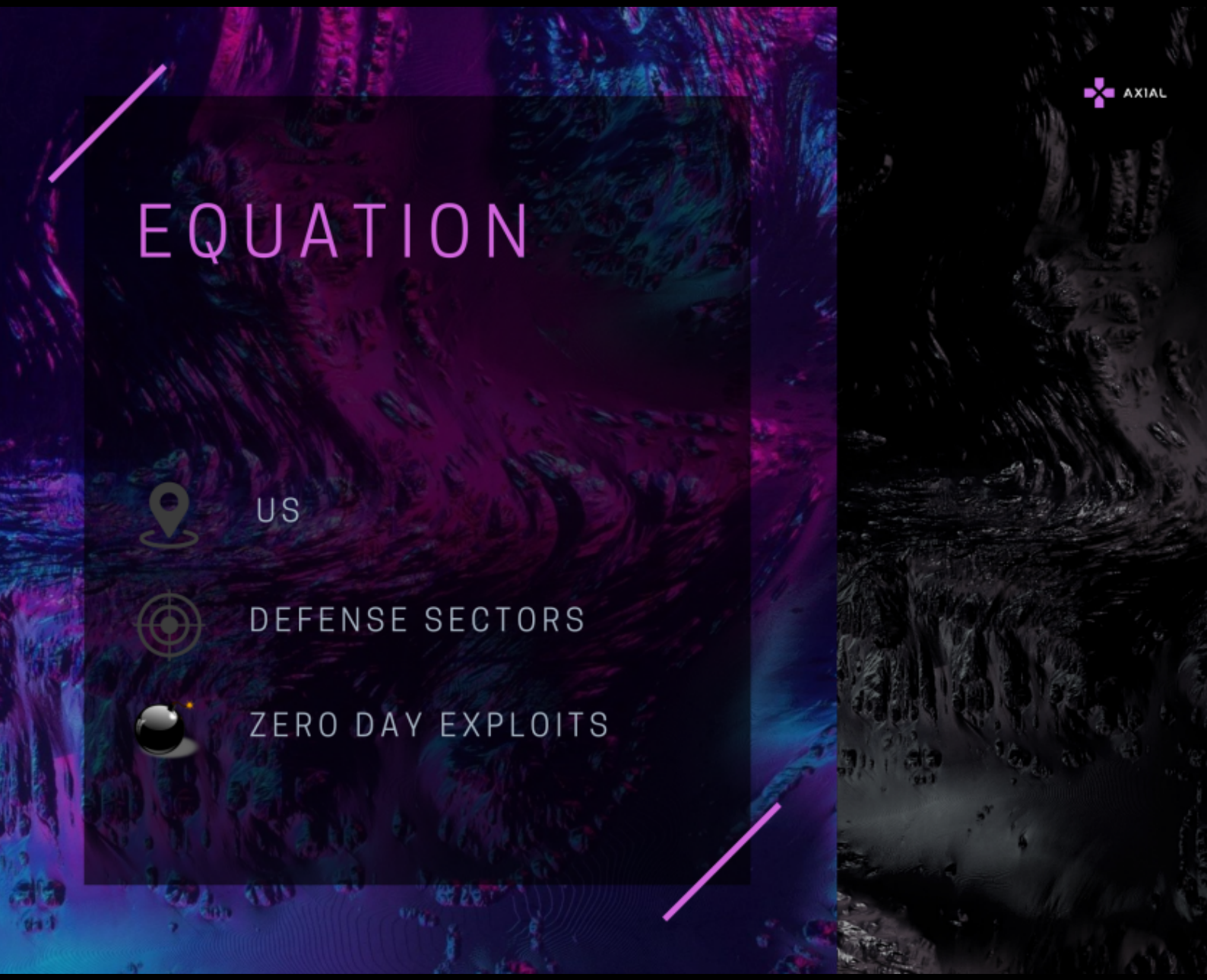
EQUATION



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON EQUATION ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Equation group which also goes by the name Tilded Team , is a state-sponsored threat group attributed to USA .

II. TARGETS

Attacks of this threat group ranges around Aerospace, Defense, Energy, Government, Media, Oil and gas, Telecommunications, Transportation and Nanotechnology, Nuclear research, Islamic activists and scholars, and companies developing cryptographic technologies.

III. METHODS USED

The methods used by this group are as follows :

• The use of virtual file systems, a feature also found in the highly sophisticated Regin malware.
• The stashing of malicious files in multiple branches of an infected computer's registry. By encrypting all malicious files and storing them in multiple branches of a computer's Windows registry, the infe ction was
impossible to detect using antivirus software.
• Redirects that sent iPhone users to unique exploit Web pages

• The use of more than 300 Internet domains and 100 servers to host a sprawling command and control infrastructure.

• An unusual if not truly novel way of bypassing code-signing restrictions in modern versions of Windows, which require that all third-party software interfacing with the operating system kernel be digitally signed by a recognized certificate authority.

IV. CAMPAIGNS

This group has been linked to the most sophisticated computer attack group in the world that developed Stuxnet and the Flame espionage malware in Operation Olympic Games .

ATTRIBUTION

Third, other Equation Group source code makes reference to "STRAITACID" and "STRAITSHOOTER." The code words bear a striking resemblance to "STRAITBIZARRE,"one of the most advanced malware platforms used by the NSA's Tailored Access Operations unit. Besides sharing the unconventional spelling "strait," Snowden-leaked documents note that STRAITBIZARRE could be turned into a disposable "shooter." In addition, the codename FOXACID belonged to the same NSA malware framework as the Grok keylogger.

The technique closely resembles one used to conceal a potentially potent warhead in Gauss,a piece of highly advanced malware that shared strong technical similarities with both Stuxnet and Flame. (Stuxnet, according to The New York Times, was a joint operation between the NSA and Israel, while Flame, according to The Washington Post, was devised by the NSA, the CIA, and the Israeli military.)

[cited from ThaiCERT]

AX1AL

V. IOCS

Hashes(SHA-1)

0044c9bfeaac9a51e77b921e3295dcd91ce3956a
06cf1af1d018cf4b0b3e6cfffca3fbb8c4cd362e
3ef06b6fac44a2a3cbf4b8a557495f36c72c4aa6
5b1efb3dbf50e0460bc3d2ea74ed2bebf768f4f7
930d7ed2bdce9b513ebecd3a38041b709f5c2990
e9537a36a035b08121539fd5d5dcda9fb6336423

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?u=29bfd981-357b-4871-ba4b-ada033ba3217