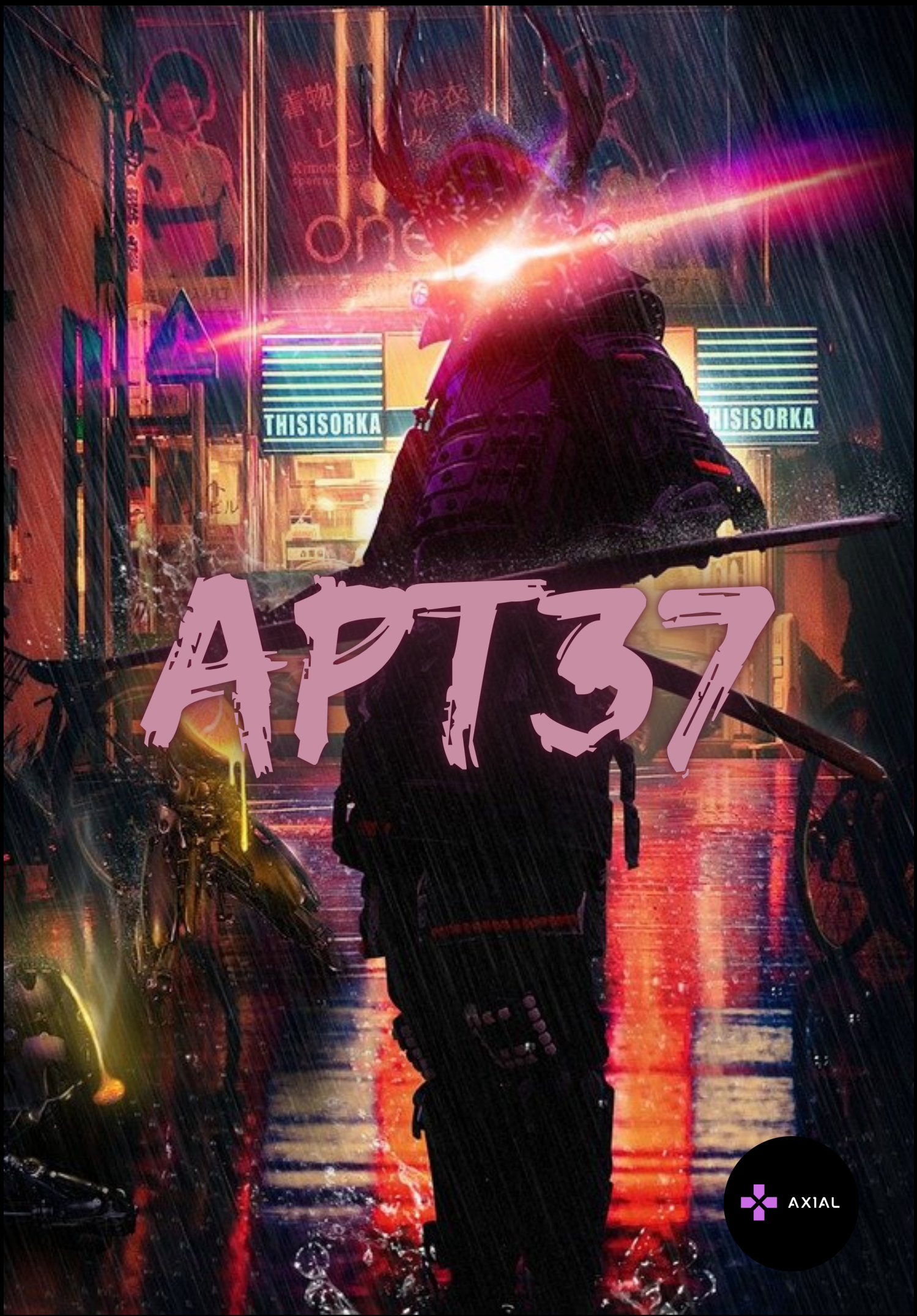
THISISORKA
APT37
AXIAL

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

-NERDS OF AX1AL

I. ABOUT

APT37 also known as Reaper, Ricochet Chollima, ScanCruft, Thallium, Group 123, RedEyes, Geumseong121, Venus 121, Hermit, ATK 4, and ITG10, is a state-sponsored threat group from North Korea that has been active since 2012. This threat group has targeted countries like China, Hong Kong, India, Japan, Kuwait, Nepal, Romania, Russia, South Korea, the UK, the USA, Vietnam with the prime motivation of Information Theft and Cyberespionage. According to FireEye, APT37's recent activity reveals that the group's operations are expanding in scope and sophistication, with a toolset that includes access to zero-day vulnerabilities and wiper malware.

III. METHODS USED

Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyber espionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately. Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adobe Flash. The group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into operations.

II. TARGET SECTORS

Reaper's observed target sectors are Aerospace, Automotive, Chemical, Financial, Government, Healthcare, High-Tech, Manufacturing, Technology, Transportation.

IV. IOC

C2

1. buttyfly.000webhostapp[.]com
2. planar-progress.000webhostapp[.]com
3. 120.192.73[.]202
4. 180.182.52[.]76

MD5

- 02681a7fe708f39beb7b3cf1bd557ee9
- C781f5fad9b47232b3606e4d374900cd
- 032ed0cd234f73865d55103bf4ceaa22
- 1f5ac2f1744ed9c3fd01fe72ee8d334f
- 4d20f7311f4f617104f559a04afd2fbf
- 03e5e566c1153cb1d18b8bc7c493025f
- C66ef71830341bb99d30964a8089a1fc
- 5999e01b83aa1cc12a2ad6a0c0dc27c3
- 4d3c34a3070643c225be1dbbb3457ad4
- f0a5385d0d9f7c546b25a7448ca5b1c9
- 8b55d52b12cf319d9785ad8eeeade5ea
- 2fdbb9a500143a2dd3d226a1cc3e45b5
- 2fdbb9a500143a2dd3d226a1cc3e45b5

V. ENGAGEMENTS

- In 2012, it was reported that Reaper has been spying on South Korean Users.
- In 2016, a South Korean web hosting company became victims of a Linux ransomware that targeted 153 of its servers. It affected websites, databases, and multimedia files of around 3.4k businesses. This was dubbed Operation Erebus.
- In March 2016, High Profile Victims were targeted using Adobe Flash Player 0day. It was dubbed Operation "Daybreak"
- In August 2016, Reaper used spear-phishing emails combined with malicious HWP documents that targeted South Korean Users. Dubbed as Operation "Golden Time". The same Attack vector resurfaced again in November, now dubbed as Operation "Evil New Year"
- In March of 2017, Reaper had gained access to remote infected systems and had wiped the first sectors of devices of South Korean Users. Dubbed as Operation "Are you Happy?" A few months later, Operation "FreeMilk" was conducted against Several Non-Korean financial institutions in which a malicious MS Office document was used. In November, Operation "North Korean Human Right" was conducted against South Korean users, using Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
- Operation "Evil New Year 2018", was an Operation targeting South Korean Users, using spearphishing emails combining them with malicious HWP documents.
- Operation "Battle Cruiser", reported in March 2018, was an ongoing operation that used the HWP document file vulnerability to perform a spear-phishing attack on users in a specific field in Korea.
- In 2019, It was discovered that APT37 was constantly trying to elaborate its attack tools as it introduced a Bluetooth harvester
- Between July and October 2019, Unit 42 observed several malware families typically associated with the APT37, targeting a US government agency.

VI. ATTRIBUTIONS

- Targeting individuals/organizations who have interest in, are directly linked to, or conduct business in North Korea
- Utilizing malicious document phishing lures containing subject matter pertaining to North Korea
- Iteratively increasing the type and complexity of their payload delivery mechanisms (from their initial use of simple Base64 strings as reported by Trend Micro, then later leveraging CARROTBAT, and now leveraging CARROTBALL)

VII. REFERENCES

- https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html
- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/erebus-linux-ransomware-impact-to-servers-and-countermeasures
- https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/
- https://unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/
- https://unit42.paloaltonetworks.com/the-fractured-statue-campaign-u-s-government-targeted-in-spear-phishing-attacks/
- https://global.ahnlab.com/global/upload/download/techreport/[AhnLab] Red_Eyes_Hacking_Group_Report (1).pdf
- https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime/