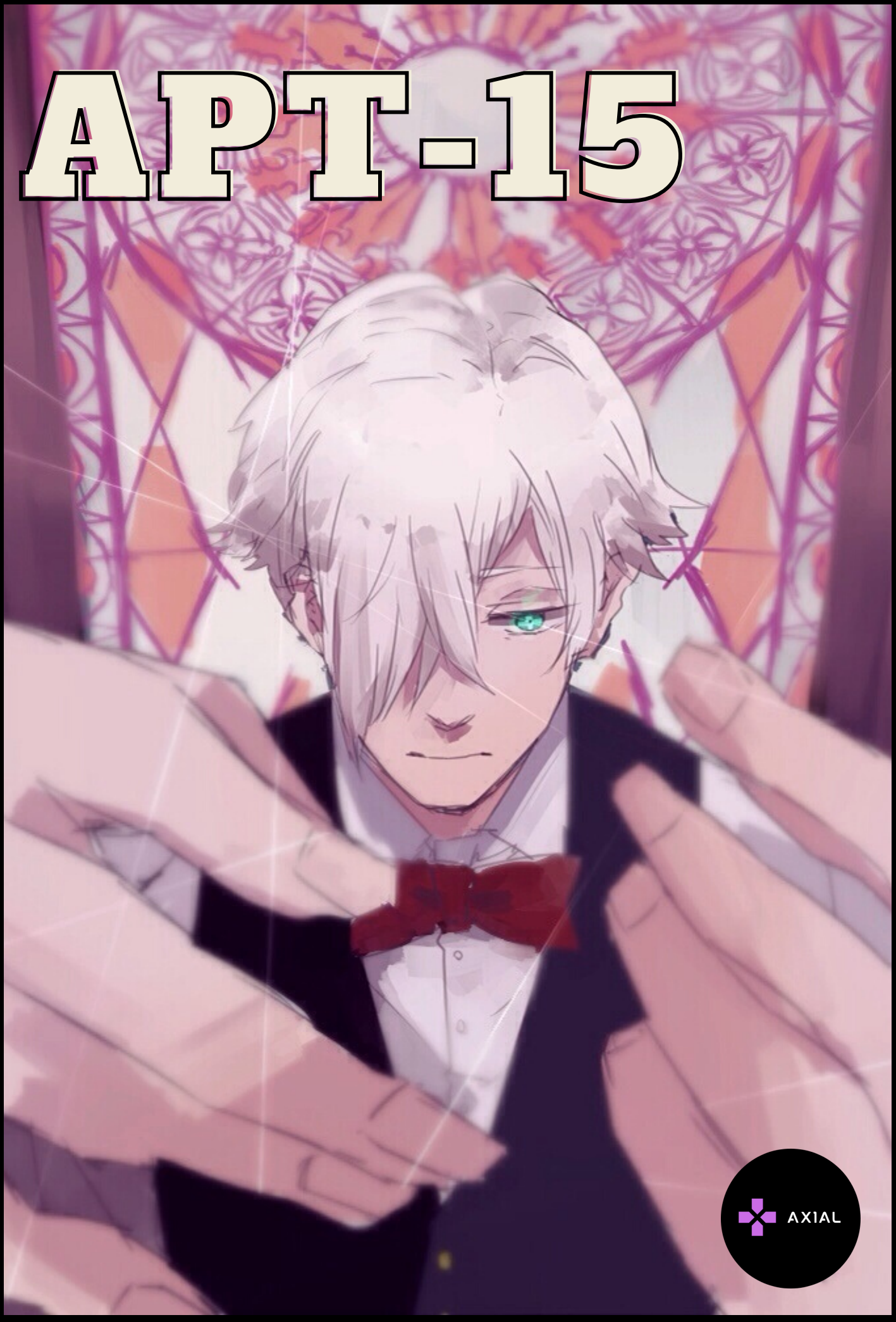
APT-15



A SURVEY ON KE3CHANG: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Ke3chang is a threat group attributed to actors operating out of China. Ke3chang has targeted several industries, including oil, government, military, and more.APT15 is also known as, Ke3chang, Mirage, Vixen Panda GREF and Playful Dragon.Analysis of the domains and IP address infrastructure used by APT15
identified a number of similar possible domains, shown at the bottom of the post. These appeared to be hosted on either Linode or Google Cloud, with a preference for using the ASN AS63949..

II. TARGET SECTORS

Ke3chang has targeted several industries, including oil, government, military, and more.Global targets in the trade, economic and
financial, energy, and military sectors in support of Chinese
government interests.APT15 was also targeting information related to UK government departments and military technology.

III. ATTRIBUTIONS

Little has been published on the threat actors responsible for Ke3chang

However, Unit 42 has recently discovered the actors have continued to
evolve their custom malware arsenal.
A new malware family named TidePool. It has strong behavioral ties to Ke3chang and is being used in an ongoing attack campaign against Indian embassy personnel worldwide.

This targeting is also consistent with previous
attacker TTPs;
Ke3chang historically targeted the Ministry of Affairs,
and also conducted several prior campaigns against India.

Attack on a company that provides a range of services to UK Government A number of sensitive documents were stolen by the attackers during the incident and it is believed APT15 was targeting information related to UK
government departments and military technology.

AX1AL

IV. METHODS USED

APT15 uses spearphising emails has a threat vector for initial hit and uses backdoors and infrastructure that is not unique to the group, making attribution challenging.
APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets

V. IOC

C&C

1. www.thehuguardian.com
2. menu.thehuguardian.com

MD5

1. a529621148e565bb2a68d89c47966be1

VI. MISCELLANEOUS

The Ke3chang hacking group makes sure to infiltrate a host and collect information about the system, such as software and hardware data. This helps the attackers to decide what would be the most efficient way to continue the operation. Other data also is exfiltrated, such as chat logs, passwords, documents, etc. Then, the attackers may opt to utilize their privileges on the compromised machine and attempt to infiltrate other potentially vulnerable systems connected to the same network.

The Ke3chang hacking group makes sure to gain persistence in the infected system. This helps them keep the planted threat active for longer periods.

VII. Referencs

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?u=110ed515-11db-4bf1-af41-a66f513ecf70
- https://www.enigmasoftware.com/ke3chang-removal
- https://www.intezer.com/blog/research/the-evolution-of-apt15s-codebase-2020/