APT-10

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-10: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

It is a state sponsored threat group based out of China . Also goes by other various names such as MenuPass Team , POTASSIUM , Cloud Hopper which has been targeting Japan , US & Europe .

II. TARGETS

Manufacturing companies, military & various government artifacts also various universities .

III. METHODS USED

- APT 10 used HAYMAKER along with the SOGU .
- APT 10 also uses BUGJUICE which is a backdoor that is executed by launching a benign file and then hijacking the search order to load a malicious dll into it.
- APT10 also uses QUASARRAT which is an open -source RAT avilable at github.
- APT 10 has also been spearphising and access to victim's networks through service providers.

.

AXIAL

IV. ATTRIBUTIONS

A group of cyber actors utilizing various tools like HAYMAKER , BUGJUICE & SNUGRIDE , QUASARRAT which is somehow serving a chinese national security goals as well as theft of confidential business data to Chinese corporations .

APT10 has targeted or compromised manufacturing companies in India, Japan and Northern Europe; a mining company in South America; and multiple IT service providers worldwide

[Cited from Fireeye]

VII. IOCS

MD5 Hashes

598FF82EA4FB52717ACAFB227C83D474"

"7D10708A518B26CC8C3CBFBAA224E032"

AF406D35C77B1E0DF17F839E36BCE630"

6EB9E889B091A5647F6095DCD4DE7C83"

566291B277534B63EAFC938CDAAB8A399E41AF7D

More IOCs :
https://github.com/jonaslejon/apt10/blob/master/hash-iocs.txt

V. REFERENCES

1. www.fireeye.com
2. www.attack.mitre.org
3. www.securelist.com
4. Kaspersky
5. JonasleJon(Github)
6. AUCERT