
AXIOM
AXIAL

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

-NERDS OF AX1AL

I. ABOUT

Axiom/Group72 is a state-sponsored threat group from the People's Republic of China that has been active since 2008. The group is sophisticated, well-funded, and possess an established, defined software development methodology. The group exclusively targets organizations based in the United States, Japan, Taiwan, and Korea.

II. TARGET SECTORS

This threat actor compromises sectors like Aerospace, Defence, Industrial, Manufacturing and Media.

III. METHODS USED

This threat actor compromises sectors like Aerospace, Defence, Industrial, Manufacturing and Media.

IV. IOC

HOSTNAME

1. fornex.uacmoscow.com
2. indian.authorizeddns.us
3. videoservice.dnset.com
4. update.mypop3.org
5. ibarakidoji.mrbasic.com
6. mn.pop-corps.com
7. jp.dynamic-dns.net
8. daum.xxuz.com
9. freemusic.zzux.com
10. likeme.myddns.com

MD5

- 5909983db4d9023e4098e56361c96a6f
- 3a3dc9cd291a79cbd5874cc787725acf
- f2b37be311738a54aa5373f3a45bbde2
- d5cf8f4c8c908553d57872ab39742c75
- 3d760b6fc84571c928bed835863fc302
- 964be19e477b57d85aceb7648e2c105d
- ed4481a9b50529bfa098c4c530e4198e
- 9f01cb61f342f599a013c3e19d359ab4
- e6aa938be4b70c79d297936887a1d9a3
- 7bb16d5c48eb8179f8dafe306fc7e2c2

V. LINKS TO OTHER THREAT GROUPS

Though both this group and Winnti Group, Blackfly, Wicked Panda use the malware Winnti, the two groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting. Could be related to APT 17, Deputy Dog, Elderwood, Sneaky Panda and/or APT 20, Violin Panda.

AX1AL

VI. ENGAGEMENTS

- Operation "SMN" is part of the coalition that includes Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity, Novetta, and Symantec. According to Operation SMN reports, Axiom is responsible for directing highly sophisticated cyber espionage against numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies worldwide from 2008 to 2014. Operation "SMN" outlined, detected, and cleaned 43,000 separate installations of Axiom tools, including 180 of their top tier implants.

VII. ATTRIBUTIONS

- Talos states that they have seen similar patterns used in domain registration for malicious domains and the same tactics being used by other State-sponsored Chinese Threat groups.

VIII. REFERENCES

- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Axiom%2C Group 72
- https://news.softpedia.com/news/Chinese-APT-Group-Axiom-Is-Very-Technical-and-Disciplined-463373.shtml
- https://www.novetta.com/wp-content/uploads/2015/01/The-ISSA-Journal-January-2015.pdf