
TG-2889
AXIAL

A SURVEY ON TG-2889: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

TG-2889 aka Cutting Kitten is a threat group originating from Iran that has been active since 2012. It is state-sponsored and has been linked to a security company called ITSecTeam. They were first seen in 2012 and were the ones behind Operation Cleaver. Over time this threat group evolved into APT-35, aka Magic Hound, Cobalt Gypsy, and Charming Kitten.

II. TARGET SECTORS

This threat group used to target Aerospace, Chemical, Defence, Education, Energy, Financial, Government, Healthcare, Telecoms and Technology sectors as well as Banks like Bank of America, CitiGroup, PNC, BB&T, Wells Fargo and HSBC.

III. METHODS USED

TG-2889 used a mix of Phishing as well as Catfishing campaigns to deliver their malware.

IV. OPERATIONS

- In 2012, It was uncovered that a threat group has been conducting significant global surveillance and infiltration campaign. Deemed as Operation "Cleaver", it was successful in evasion and successfully leveraged both publicly available and customized tools.
- In 2013, TG-2889 infiltrated the control system of a dam of NY. This sparked fears that reached to White House of a cyberwar.
- In 2015, tracking TG-2889, SecureWorks' Counter Threat Unit uncovered a network of fake LinkedIn Profiles. These profiles form a network of established LinkedIn users. CTU researchers assess with high confidence the purpose of this network is to target potential victims through social engineering.

AX1AL

V. IOC

SHA256

- 261c5f32abb8801576ce81be2c66bca564a8a28ab5ea0954bad6bac7071e299b
- 2c92da2721466bfbdaff7fedd9f3e8334b688a88ee54d7cab491e1a9df41258f

C2

1. 85.17.172.180
2. 109.172.51.147
3. 176.102.64.206
4. 185.130.226.12

VI. REFERENCES

- https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559
- https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles
- https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf