APT-29

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-29 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

APT-29 is a threat group based out of Russia and is state sponsored which focuses on information theft and espionage.

II. TARGETS

The targets of this threat group has been focused onto Defense, Energy, Government, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery onto multiple countries.

III. METHODS USED

This threat group has been using multiple methods like leveraging CVE-2013-0640 and customized backdoor written in Assembler and usage of CosmicDuke., also multiple tools and techniques like ATI-Agent, AtNow, CloudDuke, Cobalt Strike,FatDuke, GeminiDuke, HammerDuke, LiteDuke, meek, Mimikatz, MiniDuke, OnionDuke, PinchDuke, PolyglotDuke, POSHSPY, PowerDuke, RegDuke, SeaDuke, SoreFang, tDiscoverer, WellMail, WellMess, Living off the Land.

IV. CAMPAIGNS

This threat group has been involved in operation Ghost, Operation Office Monkeys and attacks on the Pentagon in the USA also has been attributed to breach of democratic national committee and running phishing campaigns in the US.

ATTRIBUTION

Cozy Bear, classified by the United States Federal Government as advanced persistent threat APT29, is a Russian hacker group believed to be associated with one or more intelligence agencies of Russia. The Dutch General Intelligence and Security Service (AIVD) deduced from security camera footage that it is led by the Russian Foreign Intelligence Service (SVR). Cybersecurity firm CrowdStrike also previously suggested that it may be associated with either the Russian Federal Security Service (FSB) or SVR.

[cited from Wiki]

AX1AL

V. IOCS

00654dd07721e7551641f90cba832e98c0acb030e2848e5efc0e1752c067ec07
0322c4c2d511f73ab55bf3f43b1b0f152188d7146cc67ff497ad275d9dd1c20f
03e9adae529155961f1f18212ff70181bde0e3da3d7f22961a6e2b1c9da2dd2e
0b8e6a11adaa3df120ec15846bb966d674724b6b92eae34d63b665e0698e0193
14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2
1fed2e1b077af08e73fb5ecffd2e5169d5289a825dcaf2d8742bb8030e487641
21129ad17800b11cdb36906ba7f6105e3bd1cf44575f77df58ba91640ba0cab9
2daba469f50cd1b77481e605aeae0f28bf14cedfcd8e4369193e5e04c523bc38
49bfff6b91ee71bbf8fd94829391a36b844ffba104c145e01c92732ada52c8ba

IPs
103.103.128[.]221
103.13.240[.]46
103.205.8[.]72
103.216.221[.]19
103.253.41[.]102
103.253.41[.]68
103.253.41[.]82
103.253.41[.]90
103.73.188[.]101
111.90.146[.]143

VI. REFRENCES

https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF

https://en.wikipedia.org/wiki/Cozy_Bear

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2029%2C%20Cozy%20Bear%2C%20The%20Dukes