SIDEWINDER

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SIDEWINDER ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Side Winder also known as APT -C-17 or RattleSnake is a threat group based out of Republic Of India which mainly focuses on Information theft and espionage.

II. TARGETS

The target/s of this threat group mainly focuses on defense and government sector of the Pakistan, China and South Asia.

.

III. METHODS USED

This threat group has been exploiting known vulnerabilities such as CVE-2017-11882, and later deploy a Powershell payload in the final stages.This threat group has also deployed malicious android application like Camero, Callcam and FileCrypt Manager which collects victim's information also leverages it's exploits in lieu of CVE-2019-2215.

IV. CAMPAIGNS

This threat group is linked to attacking android devices on March 2019 leveraging one of the known vulnerabilities.

This threat group have been linked to attacks on government and defense sector of Pakistan and China.

ATTRIBUTION

This threat group is not yet attributed being a state-sponsored threat group but links of this threat group have been found from Republic Of India, the malicious applications C&C servers leveraging CVE-2019-2215 have been suspected to be a part of Side Winder's infrastructure. Thai CERT links this threat group as originating from India.

[Cited from Trend Micro and ThaiCERT]

AX1AL

V. IOCS

Hashes

ec4d6bf06dd3f94f4555d75c6daaf540dee15b18d62cc004e774e996c703cb34 DEX AndroidOS_SWinderSpy.HRXA
a60fc4e5328dc75dad238d46a2867ef7207b8c6fb73e8bd001b323b16f02ba00 DEX AndroidOS_SWinderSpy.HRXA
0daefb3d05e4455b590da122255121079e83d48763509b0688e0079ab5d48886 ELF AndroidOS_MtkSu.A
441d98dff3919ed24af7699be658d06ae8dfd6a12e4129a385754e6218bc24fa ELF AndroidOS_BinderExp.A
ac82f7e4831907972465477eebafc5a488c6bb4d460575cd3889226c390ef8d5 ELF AndroidOS_BinderExp.A
ee679afb897213a3fd09be43806a7e5263563e86ad255fd500562918205226b8 ELF AndroidOS_BinderExp.A
135cb239966835fefbb346165b140f584848c00c4b6a724ce122de7d999a3251 ELF AndroidOS_MtkSu.A
a265c32ed1ad47370d56cbd287066896d6a0c46c80a0d9573d2bb915d198ae42 com.callCam.android.callCam2base

C&C Server:

ms-ethics.net
deb-cn.net
ap1-acl.net m
s-db.net
aws-check.net
reawk.net

VI. REFRENCES

https://www.trendmicro.com/en_us/research/20/a/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group.html

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=SideWinder%2C%20Rattlesnake