SANDCAT

AXIAL

SANDCAT

UZBEKISTAN

SAUDI ARABIA AND MIDDLE EAST

FINFISHER, CHAINSHOT AND SEVERAL 0-DAYS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

SandCat is a threat group based out of Uzbekistan and is a state sponsored threat group linked to Military Unit 02616

II. TARGETS

The target/s of this threat group mainly focuses on Saudi Arabia and the Middle East but only limited to this area they focus on basically information theft and espionage.
.

III. METHODS USED

The methods used by this groups are various 0-days and CHAINSHOT framework along with Finspy spyware. They used CVE-2019-0797 as a privilege vulnerability which exists in Windows when the Win32k component fails to properly handle objects in memory.

IV. CAMPAIGNS

This threat group has been linked to various attacks linked to Saudi Arabia.

ATTRIBUTION

This threat group is attributed to be based out of Uzbekistan and were uncovered due to bad OPSEC reasons.

[Cited from ThaiCERT]

AX1AL

V. IOCS

To be added

VI. REFRENCES

https://threatpost.com/sandcat-fruityarmor-exploiting-microsoft-win32k/142751/

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=SandCat