SHARK SPIDER

AXIAL

SHARK SPIDER

RUSSIA

Financial Sector

Shylock

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON SHARK SPIDER ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Shark Spider is a threat group based out of Russia.

II. TARGETS

The target/s of this threat group mainly focuses on financial sectors.

.

III. METHODS USED

This threat group has been using Shylock Trojan which utilizes man-in-the-browser attacks designed to pilfer banking login credentials from the PCs of clients of a predetermined list of target organizations .

The malicious applications by Side Winder threat group also leverages MediaTek-SU to get root privilege.

IV. CAMPAIGNS

This threat group is linked to attacking financial organization into various countries especially banks around the globe, it has also been linked to spreading Shylock Malware campaign through skype.

ATTRIBUTION

This threat group is not yet attributed being a state-sponsored threat group but links of this threat group have been found from Russia

[Cited from ThaiCERT]

V. IOCS

Hashes

```
4fda5e7e8e682870e993f97ad26ba6b2
bae400baf6760a1646cd44e348eea0f7
742cfd2be5d44fa072802bd4b031e818
1fd7cf2405ae599c1a91fe75912d18ff
d74f5f045c4b0f1d61746ded3a2a152e
fe17c2cddffd731ee6a34457121c6b20
a8ff900f5f3134a1f04d9217ab2d5dd0
715fb3cef70458b857bd55a0259a1265
5571be9c7b0d2e950bada71e72984e7a
72ace5e603bb4a5e2d8ef4434dc31417
9a8657a61daeafd7053017103ab53cd6
```

VI. REFRENCES

http://contagiodump.blogspot.com/2011/09/sept-21-greedy-shylock-financial.html

https://malpedia.caad.fkie.fraunhofer.de/details/win.shylock

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Shark%20Spider