GCMAN

AXIAL

APT- 18

WEKBY

CHINA

US

Gh0st RAT

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

GCMAN is a Russian based threat group which focuses on Financial destruction .

II. TARGETS

The targets of this threat group has been focused onto Russia and focuses on finance industry.

III. METHODS USED

GCMAN relied on opensoucre tools like VNC (Gui Tool used to remotly control another computer) and PuTTY (File Transfer Tool) and pentesting tools like metasploit .

They used Spearphishing Emails In Order to get into the victim network. The Spear-Phishing Emails contains Malicious (.RAR) Attachments which once opened an executable is executed and the victim got infected.

GCMAN Also Used Other Techniques like using Planting a Cron Script in the Bank Server in order to generate financial transactions at the rate of $200 per minute Other Technique is Exploiting SQL Injection In Order to get into The Victim Company and then laterally Move through the Network.

IV. CAMPAIGNS

GCMAN has been Targeting Russian Banks since 2015 using Spear phishing.

ATTRIBUTION

This threat group is focused onto Russian based financial institutions and the origin of this group is focused on Russia.

[cited from ThaiCERT]

AX1AL

V. IOCS

Hashes

b3a4096a27184df6f25a14346b506853

1a4a8aa1057411aacea0f21f442929dd

1ce5fe6a95072cdf07a922c2b481f993

8a18846e17244db9af90009ddab341ce

59254add2a5e8811570bc0b2ecf888ec

060d6ca0147d4de502749f0e68452fac

5e31d7ebfe676bdf4845b051f3932caa

fad67c9322c9302b6f3d74bd80af1f38

C2s

https://adode-update.com:443/xvbr_abgznhtovic9xmwm
http://kavupdate.net/cgi-bin/s2.cgi
http://kavupdate.net/resume.rar
https://google-src.com:443/nps1
_nmsdat9a52mphytq
https://46.28.203.60:443/fw1t
_hwytzruocih8yyws
http://banertrack.com/y2ag1985511913/ldcigar.php
198.55.119.113
200.74.240.129
94.102.63.6
5.199.165.56

VI. REFRENCES

https://apt.securelist.com/apt/gcman

https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

https://attack.mitre.org/groups/G0036/

https://exchange.xforce.ibmcloud.com/collection/Actor-GCMan-c1bbb927e46b1076352cf1ea777f088b