FIN 4

FIN 4

Romania

Mostly Pharmaceutical & Healthcare companies

Capturing Credentials

AXIAL

HAWK BASE

HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON FIN 4 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

FIN 4 is a threat group based out of Romania which focuses on obtaining access to insider information or breaking the stock prices of public companies.

II. TARGETS

The targets of this threat group has been focused on financial, healthcare and pharmaceutical based sectors.

III. METHODS USED

This group has been using VBA macros to display a dialog box and collect victim credentials, this group has also presented victims with Windows Authentication prompts to collect their credentials also they have been using .NET based keyloggers and spear phishing techniques also tools like UpDocX are being used.

IV. CAMPAIGNS

This group has been targeting public companies, over 100 in mid-2013.

ATTRIBUTION

FIN4 is attributed being an European threat group and THAICert has attributed it tobe based out of Romania.

V. IOCS

047afa3e-e080-47c7-8971-a864757934a7
982ef256-5675-4f2b-9010-d9716e89546d
b299d74c-1a6e-4291-8ed8-f0d417d573c2
1cc54e41-cd1f-4014-b45c-b4f115a4d2ce
46070bd-479c-477f-aa2c-2311199c31fd
78b9679f-2c21-47eb-ad66-851483b7837

VI. REFRENCES

https://github.com/fireeye/iocs/blob/master/FIN4/fb0699e2-23a6-40f9-bf96-4514d629eec3.ioc
https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html
https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=FIN4%2C%20Wolf%20Spider&n=1