FIN 8

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON FIN 8 ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

FIN 8 is a group focused on attacks for their own financial benefit, as opposed to APT (advanced persistent threat) groups that are focused on intelligence gathering and cyber-espionage.

II. TARGETS

The targets of this threat group has been focused on financial gain.

III. METHODS USED

This group has been breaching bank network
ks or stealing money via mass ATM cash outs, this group has also been installing malware on POS systems, this group has also been using windows 0-days and spear phishing techniques against their targets.

IV. CAMPAIGNS

This group has been targeting hospitality based industries.
This group has been targeting POS devices.

ATTRIBUTION

FIN8 has not strictly been attributed being a nation-sponsored group but the TTPs have been overlapping with other groups who are financially motivated like FIN6 and FIN7.

V. IOCS

ffebcc4d2e851baecd89bf11103e3c9de86f428fdeaf0f8b33d9ea6f5ef56685

35096c63c0ff620eb0715c4e2bbbe38350ab54d79724d1a60ae33e08ef6b8a73

a6d05539d5f79947c4c715a7138c9645eee8a8f79c0551ca020c25e86a1297a3

7cc7b0b36fd6c4af1e42931747c1e7a6f26229859f1ea7b313ce039b6aacc4c0

c240d0c33d326ed49422a8106ff82125d00f452180b4e4342c406d02d0f7e3d7

df22408833b2ae58f0d3e2fe87581be31972ef56e0ebf5efafc4e6e0341b5521

b4568f3786936cae00632cb92a421c9d90e9a076896e64611feb6c949b414180

eb6a54a0018a236c942375ee5c987e0fb01f4c3ed8b4306801084197cd0483a0

4cd86e8acd3106495ac61be242936bc6fcb55fee3fba9e2d5c93242dc6c7d86a

800615c0abac4626dc531d7b14c7360d776453ed9ad47caa7c2e138e2c1594f5

c61a5e8dc323fce6435b2f0ea45391893e2bb495a682862c2f101017d80ec37c

bf46abacce4c3b6895e4cd30156e7172598d3e3d2d45fd05bcea9160ecaf92af

d3d39452de3cfe44714a1805b5726b6df5c97ff1c81a1b729b29d3454c774bdd

0bd55c8089d5726c94f9a98221cf2ed7723a37d281173fae7cd0865c761294cb

87c8a3eb76201feb57f6ca182b6add476da7c28cdf54e86e0b83a37a742f3ba5

6049a727f96a5a089a04dc7989ad606ddfc05d08cbaca81bd9ef5be827e36a50

ed680249f0a4af4001e3cb2394f222a3ee3f4ab547fefa36b058fdbcae5e208c

4458b680f781358da2ab47e1cc43e5a4eb17e5d70825cf1c92a543b353d791b3

f73c7ed3765fec13ffd79aef97de519cfbd6a332e81b8a247fe7d1ccb1946c9c

3819baafea61af8d08709f4e9ebbbb3ffa1d9679c0673014b6cd73d788934551

09bb05993d9f6524bb081fd2f6974edca2f7a40fdd10e3466472cd04e4120577

ad578311d43d3aea3a5b2908bc6e408b499cc832723225ff915d9a7bc36e0aa4

546783504ff37a8002802b982bf3f68e7d89dddcb47a5f6f0b332980c32f3bfe

IP & Domains

8.28.175[.]68

204.155.31[.]167

138.201.44[.]3

104.193.252[.]167

104.232.34[.]36

195.54.162[.]237

aaa.stage.10556677.mx1.pdoklbr[.]com

aaa.stage.12019683.ns2.true-deals[.]com

aaa.stage.12463950.s1.rescsovwe[.]com

aaa.stage.14919005.www1.proslr3[.]com

aaa.stage.2384024.mx1.pdoklbr[.]com

aaa.stage.2940777.n1.modnernv[.]com

VI. REFRENCES

https://atr-blog.gigamon.com/2017/08/09/footprints-of-fin7-tracking-actor-patterns-iocs/

https://www.zdnet.com/article/fin8-hackers-return-after-two-years-with-attacks-against-hospitality-sector/