
FIN 7
AXIAL

A SURVEY ON FIN 7: ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

FIN7 aka ATK 32, APT-C-11, ITG14, TAG-CR1 is a Financially motivated threat group that primarily targets US retails, restaurants, and hospitality sectors since 2013. They often use PoS Malware. A portion of FIN 7 was run out of a company called Combi Security. FIN7 is sometimes referred to as Carbanak, Anunak, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately.The reports about arrests made of the mastermind of Carbanak instead of FIN7. However, security research teams keep referring to this arrest for all FIN7 activities since.

II. TARGET SECTORS

FIN 7 usually targets sectors like Gambling, Construction, Energy, Financial, Hospitality, Retail, Technology, Telecommunications and Transportation.

III. METHODS USED

FIN 7 implement sophisticated spear-phishing campaigns and distributing malware to each target through specially tailored emails. In different cases, the operators exchanged messages with their intended victims over a period of weeks before finally sending the malicious documents as attachments.

IV. COUNTER OPERATIONS

- In 2018, Three members of FIN 7 were arrested in a role for attacking over 100 US companies.
- In May 2020, a member of FIN 7 was arrested

V. IOC

SHA256

- cf86c7a92451dca1ebb76ebd3e469f3fa0d9b376487ee6d07ae57ab1b65a86f8
- c91642c0a5a8781fff9fd400bff85b6715c96d8e17e2d2390c1771c683c7ead9
- 8c00afd815355a00c55036e5d18482f730d5e71a9f83fe23c7a1c0d9007ced5a

DOMAINS

1. 185.25.48[.]186:53
2. 46.166.168[.]213:443
3. 188.165.44[.]190:53
4. 195.133.48[.]65:443
5. 195.133.49[.]73:443

AX1AL

VI. OPERATIONS

- **2017**
  - In February, FireEye identified a Spear-phishing campaign that targeted individuals involved with US Securities and Exchange Commission.
  - In March, disclosed by Kaspersky Lab and Cisco's Talos research outfit, FIN 7 made extensive use of fileless malware and known penetration testing tools and utilities to spy on organizations and move data and money off of networks.
  - In April it was found that FIN7 modified their phishing techniques to implement unique infection and persistence mechanisms. They had used implements hidden shortcut files (LNK files) to initiate the infection and VBScript functionality launched by mshta.exe to infect the victim.
  - Mandiant identified that the group leveraged an application shim database to achieve persistence on systems in multiple environments.
  - In June, FIN 7 was seen to target restaurants across US. They gained system control and install a backdoor to steal financial information at will. It incorporates some never before seen evasive techniques that allow it to bypass most security solutions – signature and behavior based.
- **2018**
  - Fifth Avenue, Saks Off 5th, and Lord & Taylor department stores—all owned by The Hudson's Bay Company—acknowledged a data breach impacting more than five million credit and debit card numbers.
  - In 2018-2019, researchers of Kaspersky Lab's GReAT analyzed various campaigns that used the same TTPs as FIN7, leading the researchers to believe that this threat actor had remained active despite the 2018 arrests.
- **2019**
  - FireEye Mandiant investigators uncovered new tools in FIN7's malware arsenal and kept pace as the global criminal operators attempted new evasion techniques. FIN 7's new tool are called BOOSTWRITE and RDFSNIFFER.
- **2020**
  - In March, TrustWave revealed that a US hospitality provider had been the target of an incredibly rare BadUSB attack. The attack happened after the company received an envelope containing a fake BestBuy gift card, along with a USB thumb drive.

VII. REFERENCES

- https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/
- https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
- https://blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign
- https://blog.morphisec.com/fin7-attacks-restaurant-industry
- https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html
- https://www.fireeye.com/blog/threat-research/2019/10/mahalo-fin7-responding-to-new-tools-and-techniques.html
- https://www.zdnet.com/article/rare-badusb-attack-detected-in-the-wild-against-us-hospitality-provider/
- https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
- https://www.bankinfosecurity.com/another-alleged-fin7-cybercrime-gang-member-arrested-a-14345