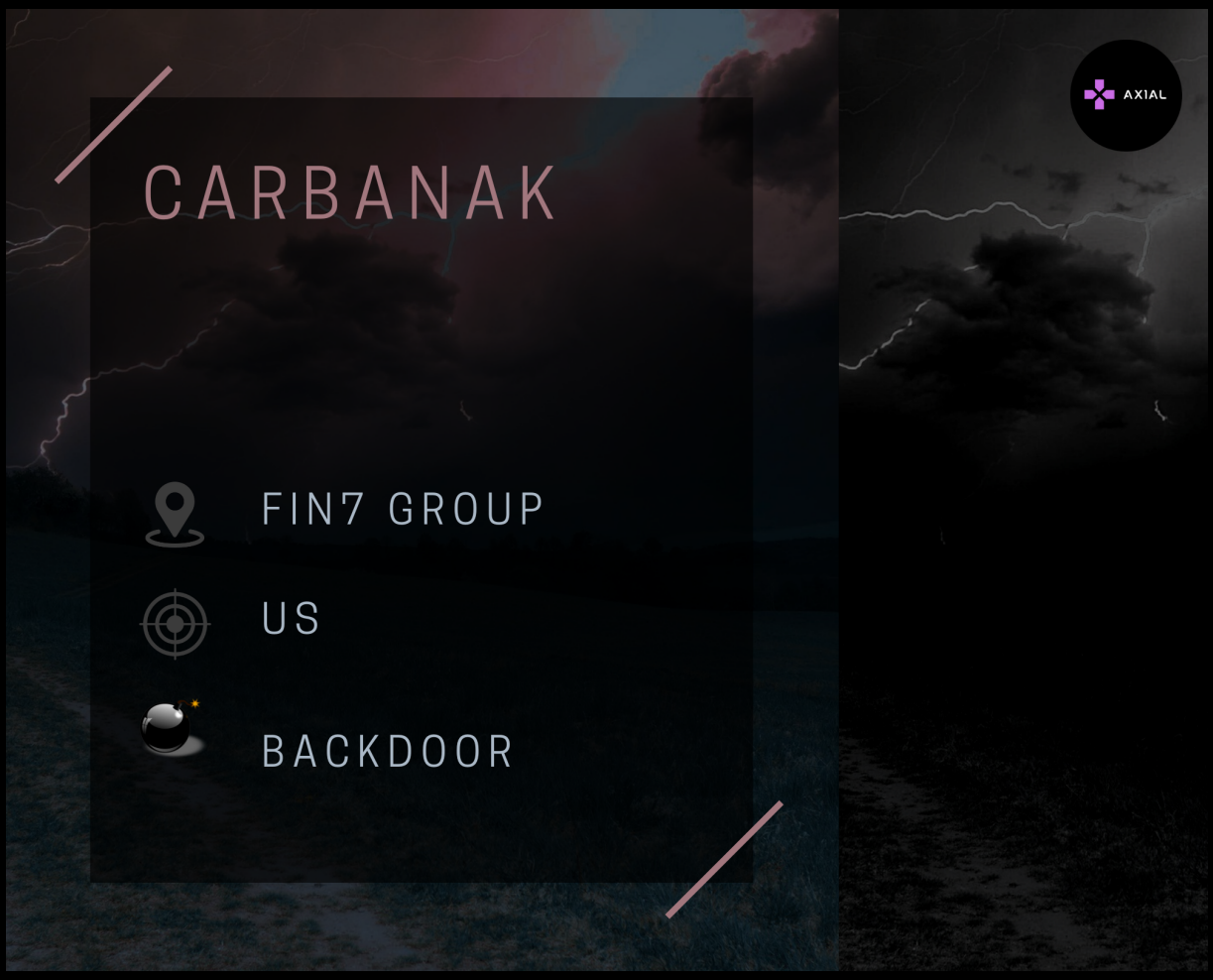
CARBANAK



HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Carbanak is a threat group that mainly targets banks for espionage and data exfiltration. The malware associated with this group is also referred to as the "Carbanak". This financially motivated threat group, dubbed as FIN7, reportedly uses the Carbanak malware in their campaigns, especially in the post exploitation phase. The group uses valid digital certificates for code signing the carbanak payload, to prove their integrity, thereby evading traditional anti-malware defenses.

II. TARGETS

Carbanak is an APT-style campaign targeting (but not limited to) financial institutions that was claimed to have been discovered in 2014 by the Russian/UK Cyber Crime company Kaspersky Lab who said that it had been used to steal money from banks.

III. METHODS USED

To begin, the criminals bought access to bank employee computers that were already compromised by massively distributed opportunistic malware. Dark Web cybercrime vendors who run immense botnets sell access to a wide selection of compromised zombies from any country. A quick search for a user's email domain can reveal the company he or she works for, allowing criminals to zero in on a target. Price tags for remote desktop-based access run no more than a few dollars.Once the Carbanak team had an initial back door into the targeted banks, it followed up with spear phishing emails designed to trick employees in the same bank and those working in other banks. The emails contained exploit-laden attachments that downloaded an insidious Trojan into the machines when they were opened by employees.

IV. CAMPAIGNS

2013 : According to kaspersky the first malicious samples were compiled in August, 2013 when the cybercriminals started to test the Carbanak malware. The first infections were detected in December, 2013.On average, each bank robbery took between two and four months, from infecting the first computer at the bank's corporate network to cashing the money out.Kaspersky believe that the gang was able to successfully steal from their first victims during the period of February-April 2014. The peak of infections was recorded in June 2014.

AX1AL

V. IOCS

MD5 Hashes

44a70bdd3dc9af38103d562d29023882
25617ce39e035e60fa0d71c2c28e1bf5
c99c03a1ef6bc783bb6e534476e5155
e741daf57eb00201f3e447ef2426142f
1e47e12d11580e935878b0ed78d2294f
ddc9b71808be3a0e180e2befae4ff433
6b51c476e9cae2a88777ee330b639166
8b3a91038ecb2f57de5bbd29848b6dc4
9f01b74c1ae1c407eb148c6b13850d28
1284a97c9257513aaebe708ac82c2e38
5ecb9eb63e8ace126f20de7d139dafe8
07b5472d347d42780469fb2654b7fc54
80dd3bd472624a01e5dff9e015ed74fd
eafba59cafa0e4fa350dfd3144e02446
2e2bc95337c3b8eb05467e0049124027
608b8bc44a59e2d5c6bf0c5ee5e1f517
370d420948672e04ba8eac10bfe6fc9c
7396ce1f93c8f7dd526eeafaf87f9c2e
2e7eec2c3e7ba29fbf3789a788b4228e
732e6d3d7534da31f51b25506e52227a
f6207d7460a0fbddc2c32c60191b6634
970056273f112900c81725137f9f8b45
81e6ebbfa5b3cca1c38be969510fae07
b789b368b21d3d99504e6eb11a6d6111
b57dc2bc16dfdb3de55923aef9a98401

C2's

http://91.207.60.68:80
http://88.150.175.102:443
http://69.195.129.72:80
http://31.131.17.127:443
http://82.163.78.188:443
http://95.215.45.228:443
http://89.46.103.42:443
http://37.235.54.48:443
http://204.155.30.100:443
http://194.146.180.40:80
http://179.43.140.82:443
http://66.55.133.86:80
http://88.198.184.241:700
http://89.144.14.65:80
http://83.166.234.250:443
http://185.180.198.2:443
http://87.98.217.9:443
http://194.146.180.44:80
http://94.156.77.149:80
http://209.222.30.5:443
http://31.7.61.136:443

TTP's

Initial Access : Spear Phishing Attachment (T1566.001)
Execution : Component Object Model and Distributed COM (T1021.003)
Execution through API (T0871)PowerShell (T1059.001)
Service Execution (T1569.002)User Execution (T1204)
Windows Management Instrumentation (T1047)
Persistence : New Service (T1543.003)
Registry Run Keys / StartupFolder (T1547)Valid Accounts (T1078)
Defense Evasion : Code Signing (T1553)
Deobfuscate/Decode Files or Information (T1140)
Masquerading (T1036)
Obfuscated Files or Information (T1027)
Process Injection (T1055)Software Packing (T1027)
Collection : Data from Local System (T1005)
Input Capture (T1056)
Screen Capture (T1113)
Command & Control (C2) : Commonly Used Port (T1436)Connection Proxy (T1090)
Standard Application LayerProtocol (T1071)
Standard Cryptographic Protocol (T1521)

VI. References / Sources

https://www.rsa.com/en-us/blog/2017-11/the-carbanak-fin7-syndicate
https://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf
https://cloudsek.com/threatintelligence/carbanak-fin7-crime-gang-threat-intel-advisory/
https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064518/Carbanak_APT_eng.pdf