Tópicos Especiais em Segurança da Informação

TP7 - Análise de códigos maliciosos

Arthur do Prado Labaki

28-06, 2022

GBC 235

Informações adicionais

Nem todos os exercícios estão com imagem aqui no relatório, mas todas as imagens integradas nesse relatório, quanto códigos, planilhas ou gifs de demonstração estão em meu repositório no GitHub abaixo.
Link do meu GitHub

Parte 1)

Para facilitar a explicação do exercício, essa primeira parte será dividia em 5, sendo uma para cada *hash* solicitado e a última para explicações gerais dos antivírus analisados. Também foi criado uma planilha para registrar as detecções doa antivírus, que está disponível no link abaixo.
Link da planilha

196eb5bfd52d4a538d4d0a801808298faadec1fc9aeb07c231add0161b416807

Esse malware é comumente conhecido como RansomExx.
Seu nome em *hash* é:

- MD5: f7c4cb42780b03303ca4b8535bb27207
- SHA-1: 6429700e978385c27d4443b1174fdb0b8940c5f3
- SHA-256: 196eb5bfd52d4a538d4d0a801808298faadec1fc9aeb07c231add0161b416807
- Vhash: 6df0735396cce17fe6a590e3e95f9069

A classe do malware é Ransomware com Cavalo de Troia.
Sua família de Ransomware é RansomExx, RansomX, Target777 ou Defray777
O tipo do arquivo binário é ELF (*Executable and Linkable Format*).
Seu tamanho é 253.59 KB (259680 bytes).
Por ser um ELF, o sistema operacional relacionado predominante é o Linux.
Esse malware foi responsável por atacar diversas empresas brasileiras, como a Renner e até o Superior Tribunal de Justiça (STJ).

cd9c621c0398dd8935890ffbe48a6cb1ebf8e7170b58b2a4981d98813d121282

Esse malware é comumente conhecido como Mirai.
Seu nome em *hash* é:

- MD5: 9f5285d74c8e7ee2e900b89f850604ba
- SHA-1: 89a18a364ca2e4dd382c57f50cdb4402b92a2bfb
- SHA-256: cd9c621c0398dd8935890ffbe48a6cb1ebf8e7170b58b2a4981d98813d121282
- Vhash: 3a9557e5312dce5056e3f79cc0a82d61

A classe do malware é Botnet focada em ataques de negação de serviços.
Ainda alguns analisadores afirmam que esse malware é Backdoor.
Sua família de Botnet/Backdoor é Mirai.1.
O tipo do arquivo binário é ELF (*Executable and Linkable Format*).
Seu tamanho é 35.30 KB (36152 bytes)
Por ser um ELF, o sistema operacional relacionado predominante é o Linux.
O malware em questão foi inicialmente usado para atacar servidores do jogo Minecraft e empresas que ofereciam proteção contra DDos para esses servidores, utilizando ataques de negação de serviços.

7786483b897971c243102c6203d0f19608524cba52136ae5fa71803e74d55825

Esse malware é comumente conhecido como GoCryptoLocker.
Seu nome em hash é:

- MD5: 8f616ddebbce71e29951a6e9472f2ea6
- SHA-1: 0394adee22cc087a07b5f661eeb008fb4083163a
- SHA-256: 7786483b897971c243102c6203d0f19608524cba52136ae5fa71803e74d55825
- Vhash: 0260f7555d14547474747az25!z

A classe do malware é Ransomware com Cavalo de Troia.
Sua família de Ransomware é GoCryptoLocker, Filecoder ou Ransom Encoder.
O tipo do arquivo binário é Win32 EXE PE (*Portable Executable*).
Seu tamanho é 2.62 MB (2749952 bytes)
Por ser um EXE, o sistema operacional relacionado predominante é o MS Windows.
Esse malware é CriptoLocker, ou seja, ele criptografa e bloqueia o acesso aos arquivos, exigindo dinheiro para o resgate deles.

a1b05e1fc423dd9540b3c34cec562626358f55213ca3b352052792eaf8a9c98a

Esse malware é comumente conhecido como Stuxnet.
Seu nome em *hash* é:

- MD5: 03dc793dcbc7f24a986d321777c3b350
- SHA-1: d9a4fcaf116641f3e107b980a18d530af1d68719
- SHA-256: a1b05e1fc423dd9540b3c34cec562626358f55213ca3b352052792eaf8a9c98a
- Vhash: 055056551d151d7bzdnz1ez8

A classe do malware é Worm com Cavalo de Troia.
Sua família de Worm é Stuxnet, NSAnti.
O tipo do arquivo binário é Win32 EXE PE (*Portable Executable*).
Seu tamanho é 505.50 KB (517632 bytes)
Por ser um EXE, o sistema operacional relacionado predominante é o MS Windows.
Pesquisando mais, Stuxnet é um Worm projetado especificamente para atacar o sistema operacional SCADA desenvolvido pela Siemens e usado para controlar as centrífugas de enriquecimento de urânio iranianas.

Analisando os antivírus

Analisando os resultados, conseguimos verificar que alguns antivírus conseguiram detectar os quatro malwares testados. Eles são:

1. Avast
2. AVG
3. BitDefender
4. DrWeb
5. Emsisoft
6. eScan
7. ESET-NOD32
8. Fortinet
9. GData
10. Ikarus
11. Kaspersky
12. MAX
13. McAfee-GW-Edition
14. Microsoft
15. Sophos
16. Tencent
17. Trellix (FireEye)

Também exitaram poucos antivírus que não conseguiram detectaram nenhum dos quatro *hashes* malignos testados. São eles:

1. Acronis (Static ML)
2. Bkav Pro
3. F-Secure
4. TACHYON

5. Zoner

Examinando esses dados, podemos concluir que grande parte dos antivírus utilizados pela ferramenta Vírus Total (VirusTotal, 2012) tem uma boa eficiência sobre esses malwares relativamente famosos, já que 17 analisadores conseguiram detectar códigos maliciosos, além de que o malware que teve menos detecções corretas (o Mirai) teve cerca de 25 detecções, o que é um número relevante.

Parte 2)

Nessa segunda parte, foi requisitado estudar os malwares, procurar e obter duas amostras de dois malwares estudados e escolhidos anteriormente. Porém, para adquirir melhor conhecimento do assunto, foi obtido um malware de cada um dos citados no exercício, somando 13 amostra das diferentes classes e famílias de malwares, que são:

Malwares citados	
Nome Comum	Classe
ILoveYou	Worm
MyDoom	Worm
Storm	Backdoor
CryptoLocker	Ransomware
WannaCry	Ransomware
CovidLock	Ransomware
LockerGoga	Ransomware
Emotet	Trojan
Petya	Ransomware
Stuxnet	Worm
Zeus	Trojan
Melissa	Virus
SQL Slammer	Worm

Algumas informações obtidas pelo Virus Share (Roberts, 2014), pelo Cuckoo online sandbox(Guarnieri et al., 2018) ou por outras fontes foram adicionadas em uma outra tabela na

mesma planilha já disponibilizada.

Analisando os binários de malwares no *Sandbox*, é possível confirmar que são códigos malicioso por diversos fatores. Um deles pode ser a nota que o próprio ambiente virtual atribui para o arquivo analisado, sendo de 0 até 10, sendo esse ultimo muito suspeito. Todos os arquivos analisados receberam nota máxima.

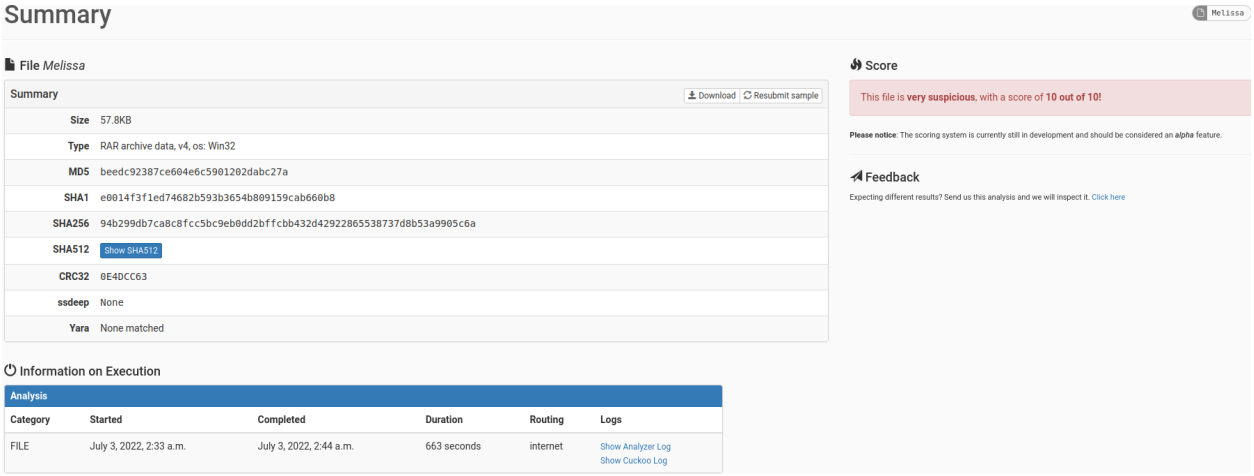

Figura 1: Resumo do malware Melissa no Cuckoo

Outra forma de analisa-los é lendo as strings deles. Nela é possível ver que diversos algumas ações dos códigos, como nos *criptomalwares*, que são malwares que criptografam os arquivos, ou *lockermalwares*, que bloqueiam o acesso do usuário aos arquivos, eles normalmente utilizam funções como *"CryptImportKey", "CryptDecrypt", "CryptGenRandom"* entre outros. Nas strings também é possível ver a linguagem que os códigos maliciosos utilizam, como *C++, HTML5, Python* e outros.

Também uma outra forma seria ver as analises de rede. Com ela é possível ver comunicações entre os malwares e outras máquinas, porém nas amostras capturadas, somente o *SQL Slammer* teve esse tipo de informação. Nele é possível ver algumas requisições HTTP para o site bdimg.share.baidu.com.

Além disso, podemos ver o *VM Memory Dump*, ou despejo da memória da maquina virtual. Isso é o processo de pegar todo o conteúdo de informação na RAM e gravá-lo em uma unidade de armazenamento, realizado pelo arquivo executado. Com ele podemo ver que tipo de processos o malware executou na maquina virtual, como *"svchost.exe", "pythonw.exe",*

"SearchProtocol"ou "explorer.exe".

Com tudo isso, usuários mais experientes devem utilizar essas ferramentas para verificar se *URLs* ou arquivos desconhecidos são maliciosos, seja subindo eles no Vírus Total para verificar a analise dos antivírus, ou até testa-lo no ambiente controlado, para ver o comportamento dele em uma máquina virtual, impedindo do malware de prejudicar o usuário. Porem, nem todos os antivírus são capazes de identificar malwares, principalmente os recentes e também existem códigos maliciosos que detectam se estão em um ambiente controlado não executando. Com isso, mesmo com as ferramentas, ainda deve-se ter muito cuidado com links e arquivos desconhecidos.

Referências

Guarnieri C. n., Tanasi A. j., Bremer J. s. e Schloesser M. r. (2018). *Cuckoo Sandbox Online*.

Roberts J.-M. (2014). *Virus share*.

VirusTotal (2012). "Virustotal-free online virus, malware and url scanner". *Online: https://www. virustotal. com/en*.