Análise do Tráfego de Rede

Bruna Almeida Osti
Rafael Cortez Sanches

Resumo

Esse trabalho tem o propósito de analisar um arquivo de captura de tráfego PCAP para identificar eventuais atividades maliciosas ocorridas em um determinado ambiente de rede. A análise mostrou a atividade de um cavalo de troia baixando código malicioso de servidores Web e enviando dados sensíveis da máquina infectada para um nó de *Command and Control* (C&C). Tanto a obtenção de binários executáveis quanto o envio de dados sensíveis foi realizada por meio do protocolo de aplicação HTTP. Também foi identificado que possivelmente uma vulnerabilidade do Microsoft Excel foi utilizada para escalar privilégios no sistema alvo e executar código como administrador.

1 Detecção de Intrusos

Para auxiliar a identificação de comportamentos maliciosos, o site *VirusTotal* foi utilizado para analisar o arquivo de tráfego fornecido para esse trabalho. Nessa análise, o site utilizou os sistemas de detecção de intrusão SNORT e Suricata para avaliar o tráfego, disponibilizando uma lista de avisos sobre atividade maliciosa nas mensagens trocadas entre os pares envolvidos. Uma vez que foi obtida uma perspectiva geral do ataque, o arquivo de tráfego fornecido foi analisado através da ferramenta *Wireshark* com o objetivo de inspecionar de forma mais apurada as mensagens de rede envolvidas no ataque.

Portanto, notamos que a melhor forma de iniciar a análise seria pela camada da aplicação, ou seja, pelas requisições http. Utilizando os filtros da ferramenta para recuperar as requisições HTTP de POST (http.request.method == "POST") e para recuperar as requisições HTTP de GET (http.request.method == "GET"). Descartamos a hipótese de dns spoofing pois os sites estão sendo requeridos ao DNS do google conhecido como 8.8.4.4.

Podemos verificar primeiramente que houveram requisições GET para alguns sites suspeitos através da Tabela 1, no qual podemos verificar que é feito o download de alguns arquivos em formatos xls, jpg e txt de diferentes servidores. Verificando os pacotes entregues podemos verificar vários textos (plain text) que não conseguimos entender o significado e alguns bem curiosos como "[SeleçãoBancoErro]".

Time	Source	Destination	Protocol	Length	Info
1.562392	192.168.115.238	200.149.77.224	HTTP	272	GET /DATA-FILES/ARQUIVO12.XLS HTTP/1.1
23.219190	192.168.115.238	66.7.200.69	HTTP	255	GET /images/get_wabs.jpg HTTP/1.1
26.057774	192.168.115.238	66.7.200.72	HTTP	54	GET /logs/logs.txt HTTP/1.1
36.437945	192.168.115.238	66.7.200.72	HTTP	54	GET /logs/logs.txt HTTP/1.1

Tabela 1: Requisições HTTP do tipo "GET"

Em seguida, podemos verificar que também houveram requisições do tipo POST após as primeiras requisições de download como demostrado na 2. Entretanto, endereçadas a um servidor diferente dos anteriores.

Nestes frames é possível visualizar que foram enviados alguns formulários com informações de login, senha, tipo de banco de dados utilizado, nome do computador, endereço de mac, nome do executável, entre outras, indo para o servidor "www.trabucar.com.br". Informações um tanto quanto suspeitas, principalmente porque há uma tag em cada arquivo com os nomes: "TransaçãoAtualizadaVersãoAtual", "TransaçãoMarcarPresençaExe"e "ITANEAviso".

Time	Source	Destination	Protocol	Length	Info
37.264539	192.168.115.238	189.126.11.82	HTTP	215	POST /images/procopspro.php HTTP/1.0 (application/x-www-form-urlencoded)
49.793605	192.168.115.238	189.126.11.82	HTTP	323	POST /images/procopspro.php HTTP/1.0 (application/x-www-form-urlencoded)
73.786949	192.168.115.238	189.126.11.82	HTTP	283	POST /images/procopspro.php HTTP/1.0 (application/x-www-form-urlencoded)

Tabela 2: Requisições HTTP do tipo "POST"

1.1 Endereços envolvidos

A tabela 3 referencia todos endereços IP envolvidos e seus respectivos nomes de domínio (quando disponíveis).

Endereço IP	**Nome de domínio**
66.7.200.72	brdotcom.com.br
66.7.200.69	www.brworks.com.br
189.126.11.82	trabucar.com.br
200.149.77.224	www.marcialemos0000.xpg.com.br
200.149.77.227	www.marcialemos0000.xpg.com.br
200.149.77.228	www.marcialemos0000.xpg.com.br
200.149.77.223	www.marcialemos0000.xpg.com.br
192.168.115.238	-

Tabela 3: Endereços de rede envolvidos no incidente

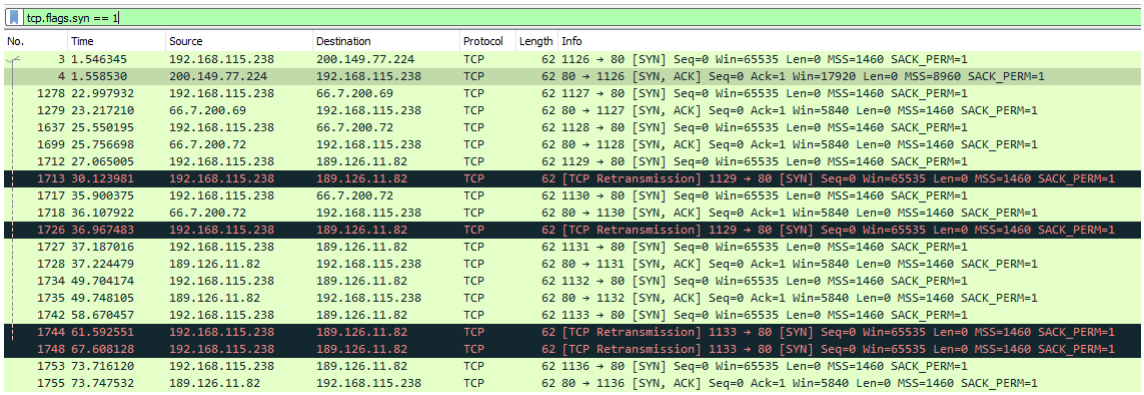
1.2 Localização dos hospedeiros atacantes

Com exceção dos endereços "66.7.200.72"e "66.7.200.69"que pertencem à HostDime (Flórida, Estados Unidos), os demais endereços são de provedores brasileiros. O endereço "192.168.115.238"é um endereço de rede local (LAN) e representa o hospedeiro infectado por um cavalo de Tróia, uma vez que dele partem as requisições HTTP identificadas nesse ataque.

1.3 Sessões TCP

Podemos observar através do filtro "tcp.flags.syn == 1"do Wireshark como mostrado na Figura 1, visualizamos pacotes com flags SYN do tcp. Como o tcp utiliza a comunicação

de 3 vias de aperto de mãos podemos verificar que ocorreram 7 requisições SYN com resposta SYN+ACK, o que corresponde à 7 sessões TCP.



tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Info
3	1.546345	192.168.115.238	200.149.77.224	TCP	62	1126 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
4	1.558530	200.149.77.224	192.168.115.238	TCP	62	80 → 1126 [SYN, ACK] Seq=0 Ack=1 Win=17920 Len=0 MSS=8960 SACK_PERM=1
1278	22.997932	192.168.115.238	66.7.200.69	TCP	62	1127 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1279	23.217210	66.7.200.69	192.168.115.238	TCP	62	80 → 1127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1637	25.550195	192.168.115.238	66.7.200.72	TCP	62	1128 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1699	25.756698	66.7.200.72	192.168.115.238	TCP	62	80 → 1128 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1712	27.065005	192.168.115.238	189.126.11.82	TCP	62	1129 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1713	30.123981	192.168.115.238	189.126.11.82	TCP	62	[TCP Retransmission] 1129 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1717	35.900375	192.168.115.238	66.7.200.72	TCP	62	1130 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1718	36.107922	66.7.200.72	192.168.115.238	TCP	62	80 → 1130 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1726	36.967483	192.168.115.238	189.126.11.82	TCP	62	[TCP Retransmission] 1129 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1727	37.187016	192.168.115.238	189.126.11.82	TCP	62	1131 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1728	37.224479	189.126.11.82	192.168.115.238	TCP	62	80 → 1131 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1734	49.704174	192.168.115.238	189.126.11.82	TCP	62	1132 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1735	49.748105	189.126.11.82	192.168.115.238	TCP	62	80 → 1132 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
1742	58.670457	192.168.115.238	189.126.11.82	TCP	62	1133 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1744	61.592551	192.168.115.238	189.126.11.82	TCP	62	[TCP Retransmission] 1133 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1748	67.608128	192.168.115.238	189.126.11.82	TCP	62	[TCP Retransmission] 1133 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1753	73.716120	192.168.115.238	189.126.11.82	TCP	62	1136 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
1755	73.747532	189.126.11.82	192.168.115.238	TCP	62	80 → 1136 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1

Figura 1: Requisições com a flag SYN e SYN+ACK

1.4 Duração do ataque

Considerando o tempo do ataque como sendo o intervalo entre o primeiro HTTP GET, que baixa o XLS malicioso para o sistema da vítima, e o último HTTP POST, o qual contém os dados sensíveis da vítima, temos:

$t_{total} = t_{POST} - t_{GET}$

$t_{total} = 73.786949s - 1,562392s$

$t_{total} = 72,2246s = 1m12s$

1.5 Comportamento do ataque

O comportamento de tráfego sugere que a máquina vítima (192.168.115.238) foi infectada por um cavalo de troia. O exemplar do código malicioso em questão se comporta como um navegador Web, fazendo requisições HTTP GET para baixar outros binários maliciosos a partir de servidores Web em endereços remotos. Uma vez que a máquina está totalmente comprometida, requisições HTTP POST são utilizadas para enviar informações sensíveis da vítima para um servidor de *Command and Control* (C&C) do atacante.

As requisições GET são enviadas aos endereços www.marcialemos0000.xpg.com.br/DATAFILES/ARQUIVO12.XLS e *www.brworks.com.br/images/get_wabs.jpg*, conforme indicado na tabela 1. Pela extensão de arquivo, o atacante tenta disfarçar os binários recuperados por essas requisições como sendo respectivamente uma planilha do Microsoft Excel (XLS) e uma imagem JPEG (JPG). Entretanto, a análise desses binários feita pelos IDS do VirusTotal mostra que eles são na verdade executáveis do Windows: "PE32 executable (GUI) Intel 80386, for MS Windows". Duas requisições GET também são feitas para recuperar um arquivo texto "logs.txt", mas essas não parecem conter informações pertinentes ao ataque. Suspeita-se que os binários recuperados por essas requisições sejam outros *malwares* utilizados para comprometer o sistema alvo para obter dados sensíveis da vítima.

Após as requisições GET, três requisições POST são enviadas para o endereço trabucar.com.br/images/procopspro.php. O formulário dessas requisições contém campos que

sugerem uma tentativa de enviar dados sensíveis da vítima para o atacante: "usuario", "senha", "macadress", "pcname", "datacadastro", "versaoatual". Outro campo recorrente é "sgdb", que possui o valor "MySQL"para todas as requisições, sugerindo que o atacante pode ter cometido um erro ortográfico ao escrever a sigla para Sistema Gerenciados de Banco de Dados (SGBD). Esses campos evidenciam que os *malwares* do atacante podem ter extraído informações de reconhecimento para um eventual ataque ao banco de dados da organização comprometida por esse incidente.

2 Análise através do VirusTotal

Utilizando a ferramenta VirusTotal foi encontrado 2 tipos de ameças, um Trojan para Win32 chamado Banbra que encontrado pelo antivírus "NANO-Antivirus", e 11 alertas de segurança pelo "Snort antivírus".

Alguns comportamentos estranhos de http foram exibidos entre os alertas, descrevendo que os arquivos que visualizamos anteriormente na requisição HTTP na verdade são executáveis do sistema Windows e não um arquivo xls e jpg como nas suas extensões.

Além disso, o relatório descrevia quais foram os problemas encontrados pelo Snort e pelo Suricata separadamente, o primeiro descrevia possíveis roubos de informações sensíveis, tráfego desconhecido, tentativa de obtenção de privilégios de administrador, violação de privacidade corporativa e detecção de Trojans de internet. De mesmo modo o Suricata encontrou possíveis violações da privacidade corporativa, Trojans de internet e tráfego ruim.

A ferramenta também exibiu a relação entre os IPs com o domínio e origem e as detecções relacionadas a cada domínio, além de sua localização como descrito na Figura 2. No qual podemos visualizar que parte dos IPs era pertencente aos EUA e parte era pertencente ao Brasil.

Contacted URLs

Scanned	Detections	URL
2017-10-28	0 / 63	http://trabucar.com.br/images/procopspro.php
2018-05-22	1 / 68	http://brdotcom.com.br/logs/logs.txt
2013-01-22	1 / 31	http://www.marcialemos0000.xpg.com.br/DATA-FILES/ARQUIVO12.XLS
2020-02-08	0 / 70	http://www.brworks.com.br/images/get_wabs.jpg

Contacted Domains

Domain	Detections	Created	Registrar
brdotcom.com.br	0 / 75	-	-
www.brworks.com.br	0 / 75	-	-
trabucar.com.br	0 / 75	-	-
www.marcialemos0000.xpg.com.br	0 / 75	-	-

Contacted IPs

IP	Detections	Autonomous System	Country
66.7.200.72	0 / 82	33182	US
66.7.200.69	0 / 75	33182	US
189.126.11.82	-	-	-
200.149.77.224	0 / 75	7738	BR
200.149.77.227	0 / 75	7738	BR
200.149.77.228	-	-	-
200.149.77.223	0 / 75	7738	BR

Figura 2: Domínios e IPs encontrados no tráfego (VirusTotal)

2.1 Execução arbitrária de código e escalada de privilégios

Em sua análise, a ferramenta SNORT aponta no arquivo XLS obtido pelo primeiro HTTP GET a presença de um *exploit* para uma vulnerabilidade das versões do Microsoft Excel 2000 SP3 e 2002 SP2, a qual permite a execução arbitrária de código como administrador. Isso permitiria uma escalada de privilégios no sistema, corroborando com o fato de que o atacante conseguiu informações de acesso para um sistema gerenciador de banco de dados.

Quanto ao binário com extensão JPG, o SNORT o acusa como abusador de uma técnica chamada *heap spraying*, utilizada para alocar memória em *heap* e diminuir os espaços de memória disponíveis para processos. Ela não é uma técnica de invasão por si só, mas ela facilita o trabalho de *malwares* que tentam inserir código executável em determinadas posições de memória, como o código malicioso do XLS anteriormente descrito. Pode ser que o atacante tenha enviado esse heap sprayer para facilitar sua escalada de privilégios no sistema.
Os respectivos alertas do SNORT estão documentados em:

- `https://www.snort.org/rule-docs/1-13570`
- `https://www.snort.org/rule_docs/1-23861`