

SRC - Projecto 2

Universidade de Aveiro
DETI

Tiago Santos, (89356), Rodrigo Rodrigues (102573)



Índice

1	Objectivos	2
2	Normal Day Analysis	2
2.1	IP's usados na rede interna	2
2.2	Volume de trafego normal entre os user internos e o servers . . .	3
2.3	Horas de funcionamento	3
3	Anomalous Behavior Detection	4
3.1	Botnet	4
3.2	C&C	5
3.3	Data Exfiltration	6
3.4	Weird Country Communication	7
4	SIEM Rules	8
4.1	Server Access Increase	8
4.2	Detecção de uploads/downloads de alto volume	8
4.3	Alto número de conexões com IPs externos	8
4.4	Acesso incomum a vários países	8
4.5	Grandes transferências de dados para países específicos	9

1 Objectivos

O objetivo do trabalho é identificar comportamentos e padrões típicos de maneira a analisar o trafego da network e detectar atividades maliciosas.

Em primeiro lugar analisamos o fluxo de um dia normal para estabelecer um comportamento típico. Em seguida, examinamos os dados do dia com anomalias de modo a encontrar BotNet, exfiltração de dados e interações de comando e controle (C&C). Com o objetivo final de criar regras SIEM com alertas para comportamentos maliciosos.

2 Normal Day Analysis

2.1 IP's usados na rede interna

		up_bytes	down_bytes	connections
dst_ip	port			
192.168.109.227	443	907794569	8385777523	79358
192.168.109.224	443	896463953	8272980644	78711
192.168.109.230	53	10883873	24992469	54359
192.168.109.225	53	10719918	24593506	53517

Figura 1: Vista global do sistema

Os servicos **227** e **224** sao responsaveis pelo maior volume de trafego indicando que sao provavelmente Web Server que gere muito trafego.

Os servicos **230** e **225** tratam do trafego na porta 53 o que pode indicar um servidor DNS

2.2 Volume de tráfego normal entre os user internos e o servers

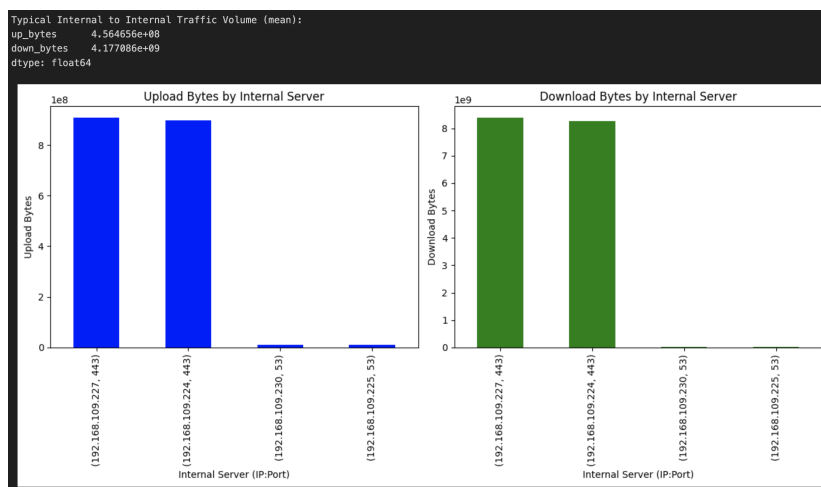


Figura 2: Tráfego

Podemos ver que o volume dos dados que usam a porta **227** e **224** são consideravelmente maiores.

2.3 Horas de funcionamento

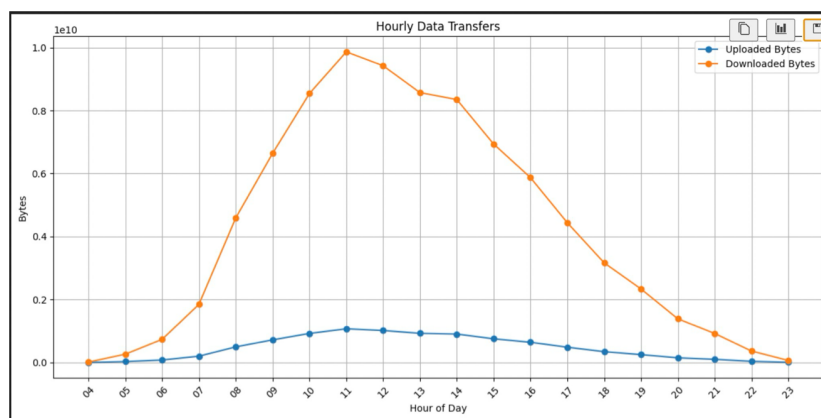


Figura 3: Transferências por hora

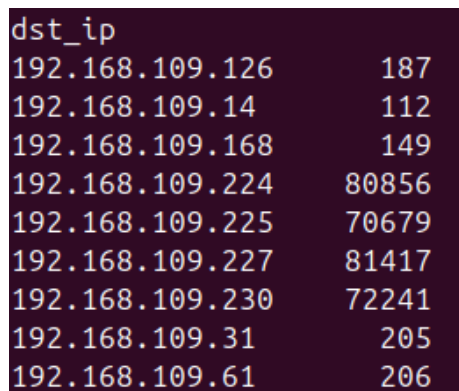
Através deste gráfico podemos observar alguns factos, peak time durante o dia e por volta das 11h. Os uploads mantêm-se bastante constantes durante o dia todo.

3 Anomalous Behavior Detection

3.1 Botnet

Um botnet é uma rede de dispositivos infectados por malware e controlados remotamente por um indivíduo ou grupo mal-intencionado. Esses dispositivos, chamados de bots, podem ser computadores, smartphones ou outros dispositivos conectados à internet. Os bots são infectados através de diversos métodos e, uma vez sob controle do invasor, podem ser usados para diversos fins maliciosos, como ataques DDoS, roubo de dados, spam e mineração de criptomoedas.

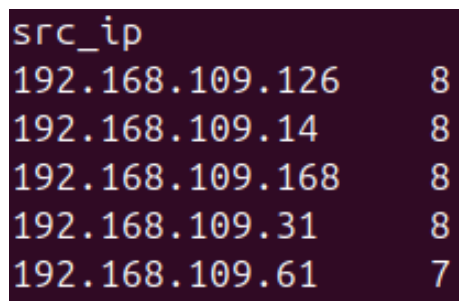
Para identificar esta atividade maliciosa, começamos por descobrir os IPs destinos privados que foram contactados e o número de conexões efetuadas.



dst_ip	
192.168.109.126	187
192.168.109.14	112
192.168.109.168	149
192.168.109.224	80856
192.168.109.225	70679
192.168.109.227	81417
192.168.109.230	72241
192.168.109.31	205
192.168.109.61	206

Figura 4: IPs de destinos privados e nº de conexões

Em seguida, encontramos os IPs de origem únicos que se comunicaram com esses IPs destinos para identificar e contar o número de conexões feitas para IPs privados únicos.



src_ip	
192.168.109.126	8
192.168.109.14	8
192.168.109.168	8
192.168.109.31	8
192.168.109.61	7

Figura 5: IPs privados únicos e nº de conexões

Como o número de conexões é alto para os IPs 192.168.109.126, 192.168.109.14, 192.168.109.168 e 192.168.109.31, há uma chance considerável de que esses IPs

sejam possíveis bots.

3.2 C&C

Para identificar atividades de Command and Control (C&C), analisamos os padrões de comunicação na rede. Utilizamos dados de comunicações internas e externas para identificar IPs que mostram um aumento significativo nas comunicações com os servidores. Primeiro, identificamos os IPs servidores observando a contagem de fluxos de comunicação interna (Figura 6).

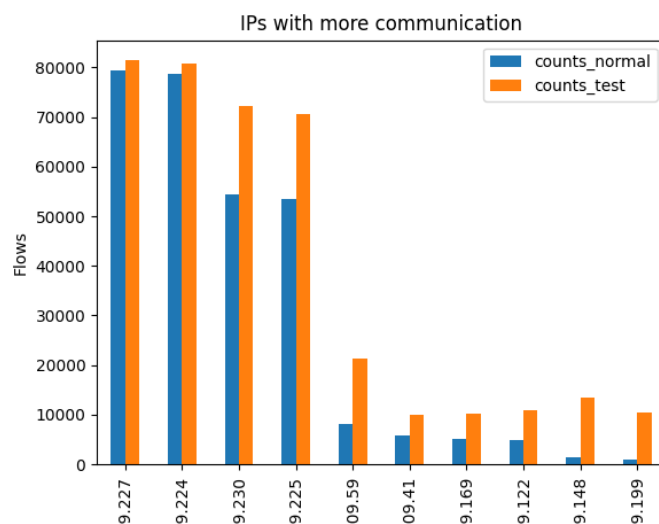


Figura 6: IPs com maior numero de comunicações

Em seguida, comparamos esses dados com as comunicações externas para identificar IPs que mostram um aumento suspeito nas comunicações com os servidores. 7

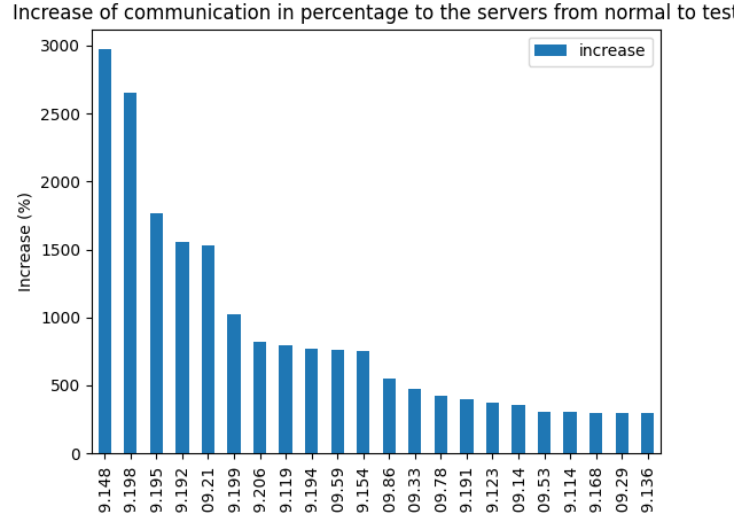


Figura 7: Aumento de comunicações em percentagem

Como podemos ver na Figura 6, não houve nenhum IP que tenha tido um "spike" no número de conexões que se torne preocupante. Na Figura 7, podemos notar que o IP 192.168.109.148 teve um aumento enorme de comunicações com o servidor, o que pode indicar uma atividade suspeita. Esse aumento significativo no tráfego de comunicação para o servidor pode ser um sinal de uma possível atividade de Command and Control (C&C).

3.3 Data Exfiltration

Detectar e prevenir a exfiltração de dados é essencial para proteger informações confidenciais e garantir a conformidade com regulamentos de privacidade e segurança. Isso geralmente envolve o monitoramento contínuo do tráfego de rede, a implementação de políticas de segurança robustas e o uso de tecnologias avançadas de detecção de ameaças.

Para identificar estas atividades calculamos a quantidade total de bytes enviados e recebidos por cada IP de origem, tanto nos dados interno-interno quanto nos dados de interno-externo.

Comparamos a média de bytes enviados e recebidos por "flow" entre os dados e identificamos potenciais candidatos à exfiltração de dados vendo aqueles IPs de origem cujo volume médio de bytes enviados ou recebidos aumentou significativamente nos dados de teste em comparação com os dados normais.

De seguida, filtramos os dados de interno-externo para identificar "flows" que correspondem a esses IPs de possam ser possíveis casos de exfiltração. Esses dados são então agregados para calcular o total de bytes enviados e recebidos por cada IP de origem suspeita. Essa análise permite-nos visualizar em 8 quais

IPs, neste case 192.168.109.196, 192.168.109.207, 192.168.109.34, de origem estão envolvidos em atividades de exfiltração de dados, destacando aqueles que apresentam os maiores volumes de bytes transferidos. Ao examinar o gráfico 8, podemos observar que os IPs 192.168.109.196, 192.168.109.207 e 192.168.109.34 são possíveis candidatos à exfiltração de dados. Eles destacam-se pelos picos significativos no volume total de bytes transferidos em comparação com os dados normais, sugerindo uma atividade anômala que merece investigação mais aprofundada.

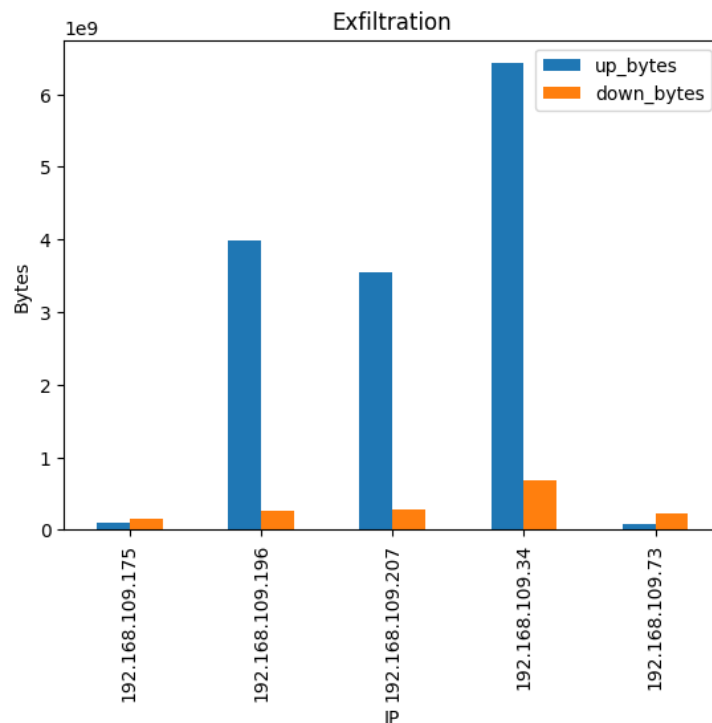


Figura 8: Resultados exfiltração de dados

3.4 Weird Country Communication

Nesta seção, nós analisamos interações com outros países, principalmente países que possam ser suspeitos devido à sua não correlação com o padrão usual de comunicações da rede. Utilizando técnicas de geolocalização de endereços IP, identificamos e investigamos conexões de rede que se dirigem a destinos em países fora das típico de operações.

Começamos por identificar no conjunto de dados quais países houve comunicações que não se encontram no ficheiro data mas sim no test. Depois descobrimos os IPs responsáveis por essas novas comunicações, obtendo: 192.168.109.18,

192.168.109.155 e 192.168.109.48 9. Estes IPs internos podem ser possíveis pontos de origem de atividades maliciosas, como exfiltração de dados sensíveis para países desconhecidos ou inesperados.

```
New countries in test data: ['IQ', 'BD', 'LU', 'IR', 'LB', 'HR', 'CZ', 'UA', 'UZ', 'RO', 'BZ', 'EE', 'VN', 'GL', 'LV', 'KG', 'MM', 'SI', 'KZ', 'PG', 'AM', 'SC', 'RU', 'DK']
IPs responsible for new countries:
src_ip      dst_ip dst_cc
Index
921072 192.168.109.18 78.41.197.41 RU
921076 192.168.109.18 194.169.85.128 RU
921078 192.168.109.18 212.184.84.150 RU
921082 192.168.109.18 185.132.240.218 RU
921092 192.168.109.18 185.254.35.7 LB
...
920664 192.168.109.155 176.119.245.13 RU
920672 192.168.109.155 45.141.87.177 RU
920674 192.168.109.155 194.35.46.13 RU
920680 192.168.109.155 5.253.166.128 RU
920682 192.168.109.155 45.147.3.250 RU
[685 rows x 3 columns]
Unique source IPs responsible for new countries:
['192.168.109.18' '192.168.109.155' '192.168.109.48']
```

Figura 9: Países estranhos e IPs responsáveis pelas comunicações

4 SIEM Rules

As regras foram implementadas no ficheiro SIEM_rules.py.

4.1 Server Access Increase

O script usa regras SIEM definidas para analisar o tráfego a detetar potenciais anomalias. Impondo um limite de 1.5x no volume de dados transferido normalmente e um limite aos países que podem aceder.

Neste projeto, implementamos uma série de regras SIEM projetadas para detectar vários tipos de anomalias de rede e potenciais ameaças à segurança.

4.2 Detecção de uploads/downloads de alto volume

Esta regra visa identificar IPs com aumentos significativos nos volumes de upload, potencialmente indicando exfiltração de dados. Ao comparar a média de bytes de upload por fluxo entre os períodos normal e de teste, sinalizamos quaisquer IPs com volumes de upload superiores a 1,5 vezes a média normal.

4.3 Alto número de conexões com IPs externos

Detecta IPs que realizam um número excessivo de conexões a endereços externos, o que pode indicar comunicação com servidores de comando e controle. Definimos um limite para o número de conexões externas e sinalizamos quaisquer IPs que excedam esse limite.

4.4 Acesso incomum a vários países

Ao usar o GeoIP para determinar os países acessados por cada IP de origem, esta regra identifica IPs que acessam um número demasiado alto de países diferentes. Definimos um limite e sinalizamos quaisquer IPs que o excedam. Esta

regra ajuda a detectar possíveis atividades de reconhecimento ou conexões com atores maliciosos estrangeiros.

4.5 Grandes transferências de dados para países específicos

Com foco na exfiltração de dados para países de alto risco, como China e Rússia, esta regra soma os bytes de upload para esses países e sinaliza quaisquer IPs que excedam um limite predefinido.