Como ler log de tráfego DNS & HTTP

Esta leitura explica como identificar ataques de força bruta usando o **tcdump**

|  |
| --- |
| 14:18:32.192571 IP **your.machine.52444 > dns.google.domain**: 35084+ A? **yummyrecipesforme.com**. (24)  14:18:32.204388 IP **dns.google.domain** > **your.machine.52444**: 35084 1/0/0 A **203.0.113.22** (40) |

A primeira sessão do arquivo de log de tráfego DNS & HTTP mostra o computador de origem (**your.machine.52444**) usando a porta **52444** para enviar uma solicitação de resolução DNS para o servidor DNS (**dns.google.domain**) para a URL de destino (**yummyrecipesforme.com**). Então a resposta retorna do servidor DNS para o computador de origem com o endereço de IP da URL de destino (**203.0.113.22**).

|  |
| --- |
| 14:18:36.786501 IP **your.machine.36086** > **yummyrecipesforme.com.http**: **Flags [S]**, seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0  14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: **Flags** **[S.]**, seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0 |

A próxima sessão mostra o computador de origem enviando uma solicitação de conexão (**Flags [S]**) partindo do computador de origem (**your.machine.36086**) usando a porta **36086** diretamente para o destino (**yummyrecipesforme.com.http**). O sufixo **.http** é o número da porta; **http** está geralmente associado com a porta **80**. A resposta mostra que o destino reconheceu e recebeu a solicitação de conexão (**Flags [S.]**). A comunicação entre a origem e o destino pretendido continua por cerca de 2 minutos, de acordo com a marcação de tempo entre este bloco (**14:18**) e a próxima solicitação de resolução DNS (veja abaixo para a marcação **14:20**).

**Códigos de Flag TCP incluem:**

**Flags [S]**  - Connection **S**tart

**Flags [F]**  - Connection **F**inish

**Flags [P]**  - Data **P**ush

**Flags [R]**  - Connection **R**eset

**Flags [.]**  - Acknowledgment

|  |
| --- |
| 14:18:36.786589 IP your.machine.36086 > **yummyrecipesforme.com.http**: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: **HTTP: GET / HTTP/1.1** |

A entrada de log com o código **HTTP: GET / HTTP/1.1** mostra que o browser está solicitando dados de **yummyrecipesforme**.**com** com o método **HTTP: GET** usando o protocolo **HTTP** versão **1.1.** Esta pode ser a solicitação de download para um arquivo malicioso.

|  |
| --- |
| **14:20**:32.192571 IP **your.machine.52444 > dns.google.domain**: 21899+ A? greatrecipesforme.com. (24)  14:20:32.204388 IP **dns.google.domain > your.machine.52444**: 21899 1/0/0 A **192.0.2.172** (40)  14:25:29.576493 **IP your.machine.56378 > greatrecipesforme.com.http**: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0  14:25:29.576510 IP **greatrecipesforme.com.http > your.machine.56378**: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0 |

Então, uma mudança brusca acontece nos logs. O tráfego é roteado do computador de origem para o servidor DNS novamente usando a porta **.52444** (**your.machine.52444 > dns.google.domain**) para fazer outra solicitação de resolução DNS. Desta vez, o servidor DNS encaminha o tráfego para um novo endereço de IP (**192.0.2.172**) e sua URL associada (**greatrecipesforme.com.http**). O tráfego muda para uma rota entre o computador de origem e o site falsificado (tráfego de saída: **IP your.machine.56378 > greatrecipesforme.com.http** e tráfego de entrada: **greatrecipesforme.com.http > IP your.machine.56378)**. Note que o número da porta (**.56378**) no computador de origem mudou de novo quando redirecionado para um novo site.

## Fontes para mais informações

* [An introduction to using tcpdump at the Linux command line](https://opensource.com/article/18/10/introduction-tcpdump): Lists several tcpdump commands with example output. The article describes the data in the output and explains why it is useful.
* [tcpdump Cheat Sheet](https://www.comparitech.com/net-admin/tcpdump-cheat-sheet/): Lists tcpdump commands, packet capturing options, output options, protocol codes, and filter options
* [What is a computer port? | Ports in networking](https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/): Provides a short list of the most common ports for network traffic and their associated protocols. The article also provides information about ports in general and using firewalls to block ports.
* [Service Name and Transport Protocol Port Number Registry](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml): Provides a database of port numbers with their service names, transport protocols, and descriptions
* [How to Capture and Analyze Network Traffic with tcpdump?](https://geekflare.com/tcpdump-examples/): Provides several tcpdump commands with example output. Then, the article describes each data element in examples of tcpdump output.
* [Masterclass – Tcpdump – Interpreting Output](https://packetpushers.net/masterclass-tcpdump-interpreting-output/): Provides a color-coded reference guide to tcpdump output