INSE 6170

Network Security Architecture and Management

Winter 2023

Firewall Configuration rules using Snort

Submitted to

Prof. Carol Fung

by

PriyaDharshan Muthu 40196410

Aravind Shankkar 40203458

Pavithran Koteeswaran 40196178

Table of Contents

I. Abstract:

In recent years, cyber attacks have become increasingly prevalent and sophisticated, posing a significant threat to organizations worldwide. As a result, the use of intrusion detection and prevention systems has become essential for network security. Snort, a widely used open-source IDS/IPS, relies on a set of rules to identify and prevent suspicious network traffic. We have created our own snort rules for the recent attacks on various organisations that were post on a malware traffic analysis website **[1].** These rules aim to detect and mitigate malicious activity, including but not limited to network scanning, exploit attempts, and data exfiltration. By providing insights into the latest threat landscape and the corresponding Snort rules, we aim to enhance the security posture of organizations and minimize the impact of cyber attacks.

II. Introduction:

In the world of cybersecurity, Intrusion Detection Systems (IDS) are an essential tool for identifying and responding to potential security threats. An IDS is a software or hardware device that monitors network traffic for suspicious activity and alerts security personnel when it detects something unusual.
There are two main types of IDS: Network-based IDS (NIDS) and Host-based IDS (HIDS). NIDS monitors network traffic, while HIDS monitors activity on individual computers or servers. Both types of IDS can be used in conjunction with other security measures, such as firewalls and antivirus software, to provide a comprehensive defense against cyber-attacks.

Snort is one of the most popular open-source IDS tools available. Snort is designed to analyze network traffic and detect suspicious patterns that may indicate a security breach. Snort works by analyzing network traffic in real-time and comparing it to a set of rules defined by the user. These rules can be customized to match specific patterns or behaviors that are indicative of an intrusion attempt or other security threat. When Snort detects a potential threat, it generates an alert that can be logged, displayed on a console, or sent to a remote monitoring system. This allows security personnel to quickly identify and respond to security incidents as they occur

Using Snort can provide a number of benefits for organizations looking to improve their network security. By detecting and responding to security threats in real-time, Snort can help prevent data breaches, network downtime, and other costly security incidents

III. Installing and Configuring Snort:

Installing and configuring Snort can be a complex process, but there are many resources available to help guide users through the setup. The first step is to download and install the Snort software on a server or dedicated hardware device. Once installed, Snort can be configured using a range of command-line options and configuration files.

IV. Snort Rules Types:

Snort rules can be classified into three types Signature-Based Rules, Protocol-Based Rules, and Anomaly-Based Rules.

Signature-Based rules are the most common type of Snort rule and are used to match patterns in network traffic. Signature-based rules can be written to match specific strings, regular expressions, or byte sequences in network packets. These rules are based on known attack patterns and are updated regularly to protect against new threats.

```
alert tcp any any -> any 80 (msg:"Web Server Attack"; content:"/cmd.exe"; nocase;
sid:100001;) [2]
```

A. Rule headers: [2]

- alert – Rule action. Snort will generate an alert when the set condition is met.
- any – Source IP. Snort will look at all sources.
- any – Source port. Snort will look at all ports.
- → Direction. From source to destination.
- $HOME_NET – Destination IP. We are using the HOME_NET value from the snort.conf file.
- any – Destination port. Snort will look at all ports on the protected network.

Protocol-Based rules are used to detect traffic that violates the protocol standards. They are based on the protocol specifications and are used to detect anomalies in network traffic.

```
alert tcp any any -> any any (msg:"TCP Null Scan"; flags:0; sid:100002;) [2]
```

Anomaly-Based rules are used to detect abnormal network behavior, such as port scanning or network probing. They are based on statistical analysis of network traffic and are used to detect patterns that deviate from the normal traffic patterns.

```
alert tcp any any -> any any (msg:"TCP SYN Flood"; flags:S; threshold: type threshold, track
by_src, count 50, seconds 10; sid:100003;) [2]
```

B. Rule Action:

In Snort, rule actions specify what happens when a rule is triggered

Alert: This is the most common action, and it generates an alert message to notify the administrator that a potential attack has been detected.

This rule generates an alert message when a TCP packet is sent from any source port to port 22 (SSH) and contains the string "SSH-" in the payload.

```
alert tcp any any -> any 22 (msg:"SSH Login Attempt"; content:"SSH-"; sid:100001;)
```

Log: This action logs the packet that triggered the rule, but does not generate an alert message.

This rule logs all TCP packets sent from any source port to port 80 (HTTP).

```
log tcp any any -> any 80 (msg:"HTTP Traffic"; sid:100002;)
```

Pass: This action tells Snort to ignore the packet and not generate any alerts or logs.

This rule tells Snort to ignore all TCP packets sent from any source port to port 53 (DNS).

```
pass tcp any any -> any 53 (msg:"DNS Traffic"; sid:100003;)
```

Drop: This action drops the packet that triggered the rule and does not generate any alerts or logs.

This rule drops all TCP packets sent from any source port to port 445 (SMB).

```
drop tcp any any -> any 445 (msg:"SMB Traffic"; sid:100004;)
```

Reject: This action is similar to "Drop," but it also sends a TCP RST (reset) packet back to the source, indicating that the connection was rejected.

This rule sends a TCP RST packet to the source IP address when a TCP packet is sent from any source port to port 22 (SSH).

```
reject tcp any any -> any 22 (msg:"SSH Reject"; sid:100005;)
```

V. Implementation:

A. Setting-Up Snort:

To set up Snort is just like any other package installation in Linux.

1. apt-get update
2. apt-get install snort

The above commands are used to update the package index files on the system, which contain information about available packages and their versions after which we can install Snort.
Once installed, it comes with its own community rules and a "**local.rules**" file in which we will write our customized rules for incoming and outgoing traffic.

B. PCAP (Packet Capture) files:

Packet Capture or PCAP (also known as libpcap) is an application programming interface (API) that captures live network packet data from OSI model Layers. Network analyzers like Wireshark create. These PCAP files can be used to view TCP/IP and UDP network packets. If you want to record network traffic then you need to create a pcap file. You can create a pcap file by using a network analyzer or packet sniffing tool like Wireshark or tcpdump. **[3]**

We have used pcap of the recent vulnerabilities and used them with snort to filter out any traffic that is similar to these headers in the packet. The snort rules generated for detecting vulnerabilities collected for the malware analysis website [1], were compared with the pcap files captured through Wireshark to detect any potential attacks.

VI. Generated Snot Rules:

1. Fake Notepad++ in a Google Ad leading to Rhadamanthys Stealer exe.

```
GET /gjntrrm/zznb2o.hgfq HTTP/1.1
Host: 162.33.178.106
User-Agent: curl/5.9
Connection: close
X-CSRF-TOKEN:
9AVz9vWrH8A/OQam/pRWLRXTUik1dOkT6q+zGWx6eioVBZpYowe4IPs0a9N955u4HvbLMGMt4
GyAFxDi9EutVA==
Cookie: CSRF-
TOKEN=9AVz9vWrH8A/OQam/pRWLRXTUik1dOkT6q+zGWx6eioVBZpYowe4IPs0a9N955u4HvbL
MGMt4GyAFxDi9EutVA==; LANG=en-US
```

```
GET /gjntrrm/zznb2o.hgfq HTTP/1.1
Host: 162.33.178.106
User-Agent: curl/5.9
```

```
Upgrade: websocket
Connection: upgrade
Sec-Websocket-Version: 13
Sec-Websocket-Key: LkFxpceAGD8MMLb
```

```
alert tcp $HOME_NET any -> any any ( msg:"Fake Notepad++ in a Google Ad leading to Rhadamanthys Stealer exe"; content:"GET /"; depth:5; content:"/"; distance:0; content:".hgfq HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"."; distance:0; content:"."; distance:1; within:3; content:"."; distance:1; within:3; content:"|0d0a|User-Agent: curl/5.9"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/[a-z]{7}\/(?=[^\n\/]*[0-9])(?=[^\n\/]*[a-z])[a-z0-9]{6}\.hgfq\x20HTTP/"; reference:url, https://www.malware-traffic-analysis.net/2023/01/03/index.html ; sid:10000001;)[4]
```

2. Brazil malspam pushing Astaroth (Guildma)

```
GET /Q13hCFaXNQ64X56/lzXQFOhWzChrNh642S5/93886/Imprimir_DACTES HTTP/1.1
Host: o6a3e.ulafeohash.world
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9
```

```
alert tcp $HOME_NET any -> any any ( msg:"Brazil malspam pushing Astaroth (Guildma)"; content:"GET /"; depth:5; content:"/"; distance:0; content:"/"; distance:0; content:"/Imprimir_DACTES HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; reference:url, https://isc.sans.edu/diary/29404 ; sid:10000002;)[5]
```

```
GET /E07sWa0JVF3yJz3/ioJFa1sroWslVs3y7I1/357247/CBM_Ref7732548 HTTP/1.1
Host: i5ai2h.azuissu.directory
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54
```

```
Accept:
\subsectiontext/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9
Cookie: pais=BR; estado=CFXX; cidade=CFXX; uid=CBM_Ref7732548
```

```
alert tcp $HOME_NET any -> any any ( msg:"Brazil malspam pushing Astaroth (Guildma)";
content:"GET /"; depth:5; content:"/"; distance:0; content:"/"; distance:0;
content:"/CBM_Ref"; distance:0; fast_pattern; content:" HTTP/1.1|0d0a|Host: "; distance:7;
within:16; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-
Insecure-Requests: "; distance:0; reference:url, https://isc.sans.edu/diary/29404 ;
sid:10000003;)[5]
```

3. Malspam Causes Infection for Agenttesla Variant, Possibly Originlogger

```
GET /sav/Ztvfo.png HTTP/1.1
Host: savory.com.bd
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"MALSPAM CAUSES INFECTION FOR AGENTTESLA
VARIANT, POSSIBLY ORIGINLOGGER"; content:"GET"; depth:3; content:"/sav/"; distance:0;
content:".png HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection:
Keep-Alive|0d0a0d0a|"; distance:0; content:!"User-Agent:"; nocase; content:!"Accept";
nocase; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/sav\/[a-zA-Z]{5}\.png\x20HTTP/";
reference:url, https://twitter.com/Unit42_Intel/status/1611379660029366273 ;
sid:10000004;)[6]
```

4. RIG Exploit Kit leading to RedLine Stealer

\su

```
alert tcp $HOME_NET any -> any any ( msg:"RIG Exploit Kit leading to RedLine Stealer";
content:"GET"; depth:3; content:" /putingods.exe HTTP/1.1|0d0a|Host: "; distance:0;
fast_pattern; content:"."; distance:0; content:"."; distance:1; within:3; content:"."; distance:1;
within:3; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; content:!"User-
Agent:"; nocase; content:!"Accept"; nocase; reference:url, https://www.malware-traffic-
analysis.net/2023/03/02/index.html ; sid:10000005;)[7]
```

5. Malspam leading to Gozi

```
GET
/drew/5gOk7Dek/zsmt20PTeCMm0SrQq7oIpio/N8KmgQk9Xu/_2BempuL1G4EvOOEJ/KQe0Q_2
F_2Bt/HkD7Doyey4O/QWsBDd8Nb9Q8HC/_2BoseBS8Ht2WmJIySdKO/9LL4jY13tXIL3pf1/WRJCq
ZKPRu2z8JC/7DUlJge_2BTbv3IbJm/rvMA3VamY/XP_2FYP87xD6pwbBXwZl/_2BwGeO_2FRTXYoS
aA2/JqNlTkyjnYeuOch0XaVfzc/9Ba2NuAhAmJcj/YiXb1_2B/Rali7NzNe6qh93JnOc_2Bcj/ItOs0DD1
t_/2FJ1Vu5lqk4Mu8K7w/LFAngLD8C/fFrfjt.jlk HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0)
Host: 62.173.140.103
Connection: Keep-Alive
Cache-Control: no-cache
```

```
GET
/drew/di_2BPScPkX8e6Hu/psCofhDu5QLI0gE/QC39CwYs1g9Bnvm4Ea/7y1p7ch9K/aa6r_2BXxtVJ
jTGTiVcu/x323A8bKKtZ8lw87fg4/f08whXRkcEciu_2FCk499Z/TVthnMyiXxZbx/Y6M18FOA/iD39fK
q3Gzai6sVk82ZLnhP/VpnZC3ICiL/ELRv_2FghhbLcBJqg/zhPmboXPKlU8/ha_2FXdFlKa/eQhgWtcG
Hyu0iR/CpIfKKX3N0JDXfN1hYLtO/ekbcdnLycjbnDdvV/5ztipipAkUXGwFK/X6d0n9wS/n.gif
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.138.138
Connection: Keep-Alive
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"Malspam leading to Gozi"; content:"GET";
depth:3; content:" /drew/"; distance:0; fast_pattern; content:" HTTP/"; distance:0;
content:"|0d0a|Host: "; distance:0; content:"."; distance:0; content:"."; distance:1; within:3;
content:"."; distance:1; within:3; content:"|0d0a|Connection: Keep-Alive"; distance:0;
content:!"Accept"; nocase; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/drew\/[a-zA-Z0-
9\/_]+\.(gif|jlk)\x20HTTP/"; reference:url,
https://twitter.com/Unit42_Intel/status/1633934017031467010 ; sid:10000006;)[8]
```

```
POST
/drew/b9Oq2cY9g/ltTm0P9gCLdTqAn36SSg/16Xtpef7wSfsQWP32lp/pzK8ZnG18hhPlqUtBqQulB
/Fyvy2dxaKbPx9/cI27MkKR/prE01xgTaX8k7iFUConsnjI/keSCZi8dZf/fTT0GqW3BXyuRP8xY/7wrgo
_2BUWeX/EDPwbaEHllX/UVr_2BB3Nj_2F3/nBvaM4mg7_2BBhdWY2XvA/parE5ep5OOllEPzt/At7
mda7YOn9AMp8/fkG7kl502sL8tzQIe9/ZmTuHX7n_2F/Ps8RrrC.bmp HTTP/1.1
```

```
Content-Type: multipart/form-data; boundary=154631768842639481601
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.138.138
Content-Length: 449
Connection: Keep-Alive
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"Malspam leading to Gozi"; content:"POST"; depth:4; content:" /drew/"; distance:0; fast_pattern; content:".bmp HTTP/"; distance:0; content:"|0d0a|Host: "; distance:0; content:"."; distance:0; content:"."; distance:1; within:3; content:"."; distance:1; within:3; content:"|0d0a|Connection: Keep-Alive"; distance:0; content:!"Accept"; nocase; reference:url, https://twitter.com/Unit42_Intel/status/1633934017031467010 ; sid:10000007;)[8]
```

```
GET /mise/Normativa.zip HTTP/1.1
Host: nhatheptienchebinhduong.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.63
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: it
```

```
alert tcp $HOME_NET any -> any any ( msg:"Malspam leading to Gozi"; content:"GET"; depth:3; content:" /mise/Normativa.zip HTTP/"; distance:0; fast_pattern; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1633934017031467010 ; sid:10000008;)[8]
```

```
GET /stilak32.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache
```

```
GET /stilak64.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
```

```
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"Malspam leading to Gozi"; content:"GET";
depth:3; content:" /stilak"; distance:0; fast_pattern; content:".rar HTTP/"; distance:2;
within:10; content:"|0d0a|Host: "; distance:0; content:"."; distance:0; content:"."; distance:1;
within:3; content:"."; distance:1; within:3; content:"|0d0a|Connection: Keep-Alive";
distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1633934017031467010 ;
sid:10000009;)[8]
```

```
GET /cook32.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache
```

```
GET /cook64.rar HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.149.243
Connection: Keep-Alive
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"Malspam leading to Gozi"; content:"GET";
depth:3; content:" /cook"; distance:0; fast_pattern; content:".rar HTTP/"; distance:2;
within:10; content:"|0d0a|Host: "; distance:0; content:"."; distance:0; content:"."; distance:1;
within:3; content:"."; distance:1; within:3; content:"|0d0a|Connection: Keep-Alive";
distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1633934017031467010 ;
sid:10000010;)[8]
```

5. Epoch 4 Emotet Activity

```
GET /wp-content/L/?160244 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: mtp.evotek.vn
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 4 Emotet Activity"; content:"GET"; depth:3; content:" /wp-content/L/?"; distance:0; fast_pattern; content:" HTTP/"; distance:6; within:6; content:"|0d0a|Connection: Keep-Alive"; distance:0; content:"|0d0a|Host: ";distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1633238684278591489 ; sid:10000011;)[9]
```

```
GET /img/PXN5J/ HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: malli.su
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity using OneNote Files (2023-03-16)"; content:"GET"; depth:3; content:" /img/"; distance:0; fast_pattern; content:"/ HTTP/"; distance:5; within:7; content:"|0d0a|Connection: Keep-Alive"; distance:0; content:"|0d0a|Host: "; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/img\/[A-Z0-9]{5}\/\x20HTTP/"; reference:url, https://twitter.com/Unit42_Intel/status/1636739251277647874 ; sid:10000012;)[10]
```

6. Epoch 5 Emotet Activity 2023-03-17

```
GET /slideshow/O1uPzXd2YscA/ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: aristonbentre.com
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity 2023-03-17"; content:"GET"; depth:3; content:" /slideshow/"; distance:0; fast_pattern; content:"/ HTTP/"; distance:0; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/slideshow\/[a-zA-Z0-9]+\/\x20HTTP/"; reference:url, https://www.malware-traffic-analysis.net/2023/03/17/index.html ; sid:10000013;)[11]
```

```
GET /i-bmail/6AfEa8G0W8NOtUh7hqFj/ HTTP/1.1
Accept: */*
```

```
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: attatory.com
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity 2023-03-17"; content:"GET"; depth:3; content:" /i-bmail/"; distance:0; fast_pattern; content:"/ HTTP/"; distance:0; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/i\-bmail\/[a-zA-Z0-9]+\/\x20HTTP/"; reference:url, https://www.malware-traffic-analysis.net/2023/03/17/index.html ; sid:10000014;)[11]
```

```
GET /uploads/ce8u7/ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: asakitreks.com
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity 2023-03-17"; content:"GET"; depth:3; content:" /uploads/"; distance:0; fast_pattern; content:"/ HTTP/"; distance:0; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/uploads\/[a-zA-Z0-9]+\/\x20HTTP/"; reference:url, https://www.malware-traffic-analysis.net/2023/03/17/index.html ; sid:10000015;)[11]
```

```
GET /files/TKK8yKdEvyYAbBE5avb/ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: bvdkhuyentanyen.vn
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity 2023-03-17";
content:"GET"; depth:3; content:" /files/"; distance:0; fast_pattern; content:"/ HTTP/";
distance:0; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: Keep-
Alive|0d0a0d0a|"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/files\/[a-zA-Z0-
9]+\/\x20HTTP/"; reference:url, https://www.malware-traffic-
analysis.net/2023/03/17/index.html ; sid:10000016;)[11]
```

```
GET /app/Ac8wwulKxqZjc/ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: bluegdps100.7m.pl
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"Epoch 5 Emotet Activity 2023-03-17";
content:"GET"; depth:3; content:" /app/"; distance:0; fast_pattern; content:"/ HTTP/";
distance:0; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Connection: Keep-
Alive|0d0a0d0a|"; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/app\/[a-zA-Z0-
9]+\/\x20HTTP/"; reference:url, https://www.malware-traffic-
analysis.net/2023/03/17/index.html ; sid:10000017;)[11]
```

7. ICEDID (bokbot) with back connect traffic and cobalt strike

```
GET / HTTP/1.1
Connection: Keep-Alive
Cookie: __gads=1883783121:1:816:109; _gid=57F51B383639;
_u=4E45494748424F52484F4F442D4443:41646D696E6973747261746F72:4131343638313132
4637343238324236; __io=21_562828852_2147444116_2496861255;
_ga=1.591597.1635208534.1066; _gat=10.0.20348.64
Host: liguspotforsit.com
```

```
alert tcp $HOME_NET any -> any any ( msg:"ICEDID (BOKBOT) WITH BACKCONNECT TRAFFIC
AND COBALT STRIKE"; content:"GET"; depth:3; content:" / HTTP/1.1|0d0a|Connection: Keep-
Alive"; distance:0; fast_pattern; content:"|0d0a|Cookie: __gads="; distance:0; content:"\;
_gid="; distance:0; content:"\; _u="; distance:0; content:"\; __io="; distance:0; content:"\;
_ga="; distance:0; content:"\; _gat="; distance:0; content:"|0d0a|Host: "; distance:0;
content:!"User-Agent:"; nocase; content:!"Accept"; nocase; reference:url,
https://twitter.com/Unit42_Intel/status/1639371567900798977 ; sid:10000018;)[12]
```

```
GET /forceupdate HTTP/1.1
Host: voiceinfosys.net
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"ICEDID (BOKBOT) WITH BACKCONNECT TRAFFIC
AND COBALT STRIKE"; content:"GET"; depth:3; content:" /forceupdate HTTP/1.1|0d0a|Host:
"; distance:0; fast_pattern; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0;
content:!"User-Agent:"; nocase; content:!"Accept"; nocase; reference:url,
https://twitter.com/Unit42_Intel/status/1639371567900798977 ; sid:10000019;)[12]
```

```
GET /es HTTP/1.1
Host: voiceinfosys.net
Accept: image/jpeg
Cookie:
wordpress_logged_in=RElESktETUZGR0NKSE1NQ0NETU5KRklPTUFISUREQVBOS0FOS0FNQkNQ
UEhPRkZFRVBBQ01HSExPQkFMRENIQktNRUpDRUNCTUFNQk1QS0xJSkRNSkRKTk5ORFBNSUxPT
kZLS09DREdPR0lIQkpJRUFOQUJMQk1LRkZISVBQSFBJSEVCQ0lET0hLTElPRkdDTUxHS05EQ0lQRE
NLSE1KQUdMTElCRENISEhGRE9LR09LQ05NSUJBT0dPRU9LSEhCRkNHR0dMRkRHRVBHTEJNS0tN
RkdLQkxLRkZFSE9CR05PRk5HTktHUElETENFQklPTkFDQkpDQU5JQkZHQkpBSg==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
Connection: Close
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"ICEDID (BOKBOT) WITH BACKCONNECT TRAFFIC
AND COBALT STRIKE"; content:"GET"; depth:3; content:" /es HTTP/1.1|0d0a|Host: ";
distance:0; fast_pattern; content:"|0d0a|Cookie: wordpress_logged_in="; distance:0;
content:"|0d0a|Connection: Close"; distance:0; reference:url,
https://twitter.com/Unit42_Intel/status/1639371567900798977 ; sid:10000020;) [12]
```

```
POST /af HTTP/1.1
Accept: */*
Host: voiceinfosys.net
Content-Type: text/plain
Cookie: __session__id=MTQ3NTQ0MzI4Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
Content-Length: 41560
Connection: Close
Cache-Control: no-cache
```

```
alert tcp $HOME_NET any -> any any ( msg:"ICEDID (BOKBOT) WITH BACKCONNECT TRAFFIC AND COBALT STRIKE"; content:"POST"; depth:4; content:" /af HTTP/"; distance:0; fast_pattern; content:"|0d0a|Host: "; distance:0; content:"|0d0a|Cookie: __session__id="; distance:0; content:"|0d0a|Connection: Close"; distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1639371567900798977 ; sid:10000021;) [12]
```

8. QAKBOT (QBOT

```
GET /Cm4z4dq.dat HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.2673
Host: 104.225.129.114
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"QAKBOT (QBOT), OBAMA247 DISTRIBUTION TAG"; content:"GET /"; depth:5; content:".dat HTTP/"; distance:7; within:10; fast_pattern; content:"|0d0a|Host: "; distance:0; content:"."; distance:0; content:"."; distance:1; within:3; content:"."; distance:1; within:3; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; content:!"Accept"; nocase; reference:url, https://twitter.com/Unit42_Intel/status/1643011286618259464 ; sid:10000022;) [13]
```

```
GET /dHJw183la23jm?q=9250194086 HTTP/1.1
Host: lbbyqrluzu.cracknight.ru
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

```
alert tcp $HOME_NET any -> any any ( msg:"USPS-THEMED EMAIL PUSHES NETSUPPORT RAT"; content:"GET /"; depth:5; content:"?"; distance:0; content:"="; distance:0; content:" HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; pcre:"/^GET\x20(http(s)?:\/\/[^\s\/]+)?\/(?=[^\n\/]*[0-9])(?=[^\n\/]*[a-zA-Z])[a-zA-Z0-9]{13,15}\?[a-z]\=[0-9]{10}\x20HTTP/"; reference:url, https://twitter.com/Unit42_Intel/status/1608185209329008641 ; sid:10000023;)[14]
```

```
GET /wp/ HTTP/1.1
Host: www.patrickforeilly.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

```
alert tcp $HOME_NET any -> any any ( msg:"USPS-THEMED EMAIL PUSHES NETSUPPORT RAT"; content:"GET"; depth:3; content:" /wp/ HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1608185209329008641 ; sid:10000024;) [14]
```

```
GET /index/index.php HTTP/1.1
Host: 1otal.com
Connection: Keep-Alive
```

```
alert tcp $HOME_NET any -> any any ( msg:"USPS-THEMED EMAIL PUSHES NETSUPPORT RAT"; content:"GET"; depth:3; content:" /index/index.php HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0; content:!"User-Agent:"; nocase; content:!"Accept"; nocase; reference:url,https://twitter.com/Unit42_Intel/status/1608185209329008641; sid:10000025;)

alert tcp $HOME_NET any -> any any ( msg:"USPS-THEMED EMAIL PUSHES NETSUPPORT RAT"; content:"GET"; depth:3; content:" /index/index.php HTTP/1.1|0d0a|Host: "; distance:0;
 fast_pattern; content:"|0d0a|Connection: Keep-Alive|0d0a0d0a|"; distance:0;
content:!"User-Agent:"; nocase; content:!"Accept"; nocase; reference:url,
https://twitter.com/Unit42_Intel/status/1608185209329008641 ; sid:10000025;) [14]
```

```
POST http://89.185.85.44/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    22
Host: 89.185.85.44
Connection: Keep-Alive

CMD=POLL
INFO=1
ACK=1
```

```
alert tcp $HOME_NET any -> any any ( msg:"USPS-THEMED EMAIL PUSHES NETSUPPORT
RAT"; content:"POST"; depth:4; content:" http://"; distance:0; content:"/fakeurl.htm HTTP/";
distance:0; fast_pattern; content:"Host: "; distance:0; content:"."; distance:0; content:".";
distance:1; within:3; content:"."; distance:1; within:3; content:"Connection: Keep-Alive";
distance:0; reference:url, https://twitter.com/Unit42_Intel/status/1608185209329008641 ;
sid:10000026;) [14]
```

9. ICEDID (BOKBOT) infection with cobalt strike

```
GET /download/x64.dll HTTP/1.1
Connection: Keep-Alive
Host: 209.182.227.138
```

```
alert tcp $HOME_NET any -> any any ( msg:"ICEDID (BOKBOT) INFECTION WITH COBALT
STRIKE"; content:"GET"; depth:3; content:" /download/x64.dll HTTP/"; distance:0;
fast_pattern; content:"|0d0a|Connection: Keep-Alive"; distance:0; content:"|0d0a|Host: ";
distance:0; content:"."; distance:0; content:"."; distance:1; within:3; content:"."; distance:1;
within:3; content:!"User-Agent:"; nocase; content:!"Accept"; nocase; reference:url,
https://twitter.com/Unit42_Intel/status/1606013040599699476 ; sid:10000027;) [15]
```

```
GET /elii/pulemtaevtot HTTP/1.1
```

```
Host: sapplus.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.42
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

```
alert tcp $HOME_NET any -> any any ( msg:"BB02 QAKBOT (QBOT) INFECTION"; content:"GET"; depth:3; content:" /elii/pulemtaevtot HTTP/1.1|0d0a|Host: "; distance:0; fast_pattern; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; reference:url, https://www.malware-traffic-analysis.net/2022/10/14/index.html ; sid:10000028;) [16]
```

```
GET /elii/Orig1510220021.zip HTTP/1.1
Host: sapplus.net
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 Edg/106.0.1370.42
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://sapplus.net/elii/pulemtaevtot
Accept-Encoding: gzip, deflate
Accept-Language: en
Cookie: PHPSESSID=0b2e21de80f9464098f18b90007961ab
```

```
alert tcp $HOME_NET any -> any any ( msg:"BB02 QAKBOT (QBOT) INFECTION"; content:"GET"; depth:3; content:" /elii/Orig"; distance:0; fast_pattern; content:".zip HTTP/1.1|0d0a|Host: "; distance:0; content:"|0d0a|Connection: keep-alive"; distance:0; content:"|0d0a|Upgrade-Insecure-Requests: "; distance:0; reference:url, https://www.malware-traffic-analysis.net/2022/10/14/index.html ; sid:10000029;) [16]
```

10. Files for An ISC Diary (Matanbuchus with Cobalt Strike)

```
POST /KkfUWR/kFAWCs/requets/index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft
Outlook 16.0.5197; ms-office; MSOffice 16)
Host: telemetryservic.com
Content-Length: 607
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-RUS
```

ev=eyIzQ0VrIjoicnJsTGtSR2p3c0ZqSk5maEJ5Q1J3dXdVOTdRbitNdzZqdHBVS29Fbm5QSUtuTi96R
09IS3B3PT0iLCIzZmUxMSI6IjMrWUd4QT09IiwiM203eCI6InNxUmFoZz09IiwiRFMyeCI6IjBlTWZ0a
FQvIiwiRUxqIjoicFpVUHhRPT0iLCJFbzYiOiJwckJOblJqbiIsIkZ0byI6IjB3PT0iLCJMb3MiOlsib085cWh
EcjcvYUlrSGZUd0NULzM0dmQyMU1WY2lvMTQ1T29sQWJnbSJdLCJOU2V5RFgiOiJxWVJhalRuVCI
sIlE2WDYiOiJxSmxzdlNuTzNhRT0iLCJWeiI6InBPMWpveFRsOUljMEZPVEFHM3VTd0pJQ3F0OTRwS
ng4eU9CSFcvOFh4TmM9IiwiY0JGIjoiMStjU3hENm0xdGx1VmZ5K1dqcm90b0E9IiwiZjFkYSI6InU0
dHd1aTdDeEsxdUkvcz0iLCJ0VyI6Im81SnN2eW5Fd01VS1U0dWpWRitmIiwid1A2Ijoia2VZUndGTzc
iLCJ6a0M3IjoiaUxsTW5RbnUvWUVnRmRlOUZtMm01dz09In0=

```
alert tcp $HOME_NET any -> any any ( msg:"FILES FOR AN ISC DIARY (MATANBUCHUS WITH
COBALT STRIKE)"; content:"POST /"; depth:6; content:"/"; distance:0;
content:"/requets/index.php HTTP/"; distance:0; fast_pattern; content:"|0d0a|Host: ";
distance:0; content:!"Connection:"; nocase; reference:url,
https://twitter.com/Unit42_Intel/status/1537904451108818946 ; sid:10000030;)[17]
```

```
GET /rmaS/Es.png HTTP/1.1
Host: slgemseller.com
User-Agent: curl/7.79.1
Accept: */*
```

```
alert udp $HOME_NET any -> any 53 (msg:"DNS Traffic to (communicationreporting.com) for
Cobalt Strike"; content:"|01|"; offset:2; depth:1; content:"|00 01 00 00 00 00 00|";
distance:1; within:7; content:"|16|communicationreporting|03|com|00|"; nocase;
distance:0; fast_pattern; reference:url,
https://twitter.com/Unit42_Intel/status/1537904451108818946 ; sid:10000032;)[17]
```

Reference

[1] https://www.malware-traffic-analysis.net/

[2] https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/

[3] https://www.comparitech.com/net-admin/pcap-guide/

[4] https://www.malware-traffic-analysis.net/2023/01/03/index.html

[5] https://isc.sans.edu/diary/29404

[6] https://twitter.com/Unit42_Intel/status/1611379660029366273

[7] https://www.malware-traffic-analysis.net/2023/03/02/index.html

[8] https://twitter.com/Unit42_Intel/status/1633934017031467010

[9] https://twitter.com/Unit42_Intel/status/1633238684278591489

[10] https://twitter.com/Unit42_Intel/status/1636739251277647874

[11] https://www.malware-traffic-analysis.net/2023/03/17/index.html

[12] https://twitter.com/Unit42_Intel/status/1639371567900798977

[13] https://twitter.com/Unit42_Intel/status/1643011286618259464

[14] https://twitter.com/Unit42_Intel/status/1608185209329008641

[15] https://twitter.com/Unit42_Intel/status/1606013040599699476

[16] https://www.malware-traffic-analysis.net/2022/10/14/index.html

[17] https://twitter.com/Unit42_Intel/status/1537904451108818946