Internal Threat Advisory: Rules for ‘itsoknoproblembro’

[CONFIDENTIAL]

GSI ID - 1055
Risk Factor - HIGH

Summary

This advisory contains fingerprinted IDS signatures in snort format. These are associated with the tools suite behind recent public DDoS attack campaigns that targeted multiple critical infrastructures with unprecedented levels of malicious traffic. We analyzed the versions of files that were most frequently used during our research into compromised Tier-1 servers.

Fingerprinted Signatures

- stcp.php
- stpf.php
- stcurl.php
- rp.php
  - post.pl
  - get.pl
- kamikaze
- amos mode

Recommended Mitigation: Detection against DDoS attacks (Snort Rules)

Description: This section contains snort rules for each file type listed above to include additional variants in some cases. When implemented within your own IDS infrastructure, the corresponding rule message logs will contain the filename being used to generate a particular DDoS attack vector.

stcp.php

```
alert TCP $EXTERNAL_NET any -> $HOME_NET 53 (msg:"stcp.php UDP PORT 53 Flood";\
content: "|4141 4141 4141 4141 4141 4141 4141 4141|"; offset: 0; \
threshold: type threshold, track by_src, count 5, seconds 1; \
reference:itsoknoproblembro; sid:100000001; rev:1;)

alert TCP $EXTERNAL_NET any -> $HOME_NET 80 (msg:"stcp.php UDP PORT 80 Flood";\
content: "|4141 4141 4141 4141 4141 4141 4141 4141|"; offset: 0; \
threshold: type threshold, track by_src, count 5, seconds 1; \
reference:itsoknoproblembro; sid:100000002; rev:1;)

alert TCP $EXTERNAL_NET any -> $HOME_NET 80 (msg:"stcp.php UDP PORT 443 Flood";\
content: "|4141 4141 4141 4141 4141 4141 4141 4141|"; offset: 0; \
threshold: type threshold, track by_src, count 5, seconds 1; \
reference:itsoknoproblembro; sid:100000003; rev:1;)

alert TCP $EXTERNAL_NET any -> $HOME_NET any (msg:"stcp.php TCP Flood pcre - more processor intensive";\
content: "|41|"; offset: 0; \
pcre: "/\x41$/" ;\
threshold: type threshold, track by_src, count 10, seconds 1; \
reference:itsoknoproblembro; sid:100000004; rev:1;)
```

stpf.php

```
alert UDP $EXTERNAL_NET any -> $HOME_NET 53 (msg:"stpf.php UDP PORT 53 Flood";\
content: "|4141 4141 4141 4141 4141 4141 4141 4141|"; offset: 0; \
threshold: type threshold, track by_src, count 5, seconds 1; \
reference:itsoknoproblembro; sid:100000005; rev:1;)

alert UDP $EXTERNAL_NET any -> $HOME_NET 80 (msg:"stpf.php UDP PORT 80 Flood";\
content: "|4141 4141 4141 4141 4141 4141 4141 4141|"; offset: 0; \
threshold: type threshold, track by_src, count 5, seconds 1; \
reference:itsoknoproblembro; sid:100000006; rev:1;)

alert UDP $EXTERNAL_NET any -> $HOME_NET any (msg:"stpf.php UDP Flood pcre - more processor intensive";\
content: "|41|"; offset: 0; \
pcre: "/\x41$/" ;\
threshold: type threshold, track by_src, count 10, seconds 1; \
reference:itsoknoproblembro; sid:100000007; rev:1;)
```

stpf.php - ethernet

```
alert UDP $EXTERNAL_NET any -> $HOME_NET any (msg:"stpf.php UDP Flood pcre - More
Processor Intensive";\
content: "|41|"; offset: 0; \
pcre: "/\x41$/" ;\
threshold: type threshold, track by_src, count 10, seconds 1; \
reference:itsoknoproblembro; sid:100000008; rev:1;)
```

stcurl.php

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $ HTTP_PORTS (msg:"stcurl.php GET
Flood";\
content:"GET"; offset: 0”;\
content:"HTTP/1.1|0d0a|Host\: "; \
content: "|0d0a|Accept\: */*|0d0a||0d0a|";\
reference:itsoknoproblembro; sid:100000009; rev:1")
```

rp.php - get.pl

```
alert TCP $EXTERNAL_NET any -> $HOME_NET any (msg:"rp.php get.pl";\
content: "GET http\://"; nocase; \
content: "HTTP/1.1|0d0a|TE\: deflate,gzip\;q=0.3|0d0a|Connection\: Keep-Alive, Keep-Alive,
Keep-Alive, TE, close|0d0a|Cache-Control\: no-cache|0d0a|Cache-Control\: no-cache|0d0a|
Cache-Control\: no-cache|0d0a|Accept\: */*|0d0a|Accept\: */*|0d0a|Accept\: */*|0d0a|Accept-
Encoding\: |0d0a|Accept-Encoding\: |0d0a|Accept-Encoding\: |0d0a|Accept-Language\: en-
gb,en-us,fr-po,ch-jp,kr-us|0d0a|Accept-Language\: en-gb,en-us,fr-po,ch-jp,kr-us|0d0a|Accept-
Language\: en-gb,en-us,fr-po,ch-jp,kr-us|0d0a|Host\:"; \
content: "|0d0a|User-Agent\: Mozilla/5.0 (Windows\; U\; Windows NT 6.1\; en-US\; rv\:1.9.2.6)
Gecko/20100625 Firefox/3.6.6|0d0a|Content-Type\: application/x-www-form-urlencoded|0d0a|
Content-Type\: application/x-www-form-urlencoded|0d0a|Content-Type\: application/x-www-
form-urlencoded|0d0a||0d0a|"; \
reference:itsoknoproblembro; sid:10000010; rev:1;)
```

rp.php - post.pl

```
alert TCP $EXTERNAL_NET any -> $HOME_NET any (msg:"rp.php post.pl";\
content: "POST http\://"; nocase;  \
content: " HTTP/1.1|0d0a|TE\: deflate,gzip\;q=0.3|0d0a|Connection\: Keep-Alive, TE, close|
0d0a|Cache-Control\: no-cache|0d0a|Accept\: */*|0d0a|Accept-Encoding\: |0d0a|Accept-
Language\: en-gb,en-us,fr-po,ch-jp,kr-us|0d0a|Host\: "; \
content: "User-Agent\: Mozilla/5.0 (Windows\; U\; Windows NT 5.1\; en-US\; rv\:1.8.0.5) Gecko/
20060719 Firefox/1.5.0.5|0d0a|Content-Length\: "; \
content: "Content-Type\: application/x-www-form-urlencoded|0d0a||0d0a|" ; \
reference:itsoknoproblembro; sid:10000011; rev:1;)
```

kamikaze (without cURL)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80,443 (msg:"KAMIKAZE GET FLOOD
attack"; flow:established,to_server";\
content:"GET"; offset: 0";\
content:"HTTP/1.1|0d0a|Host\: “;\
content: “User-Agent\: "; \
content:"Accept\: */*"|0d0a|Accept-Language\: en-us,en\;q=0.5|0d0a|Accept-Encoding\: deflate|
0d0a|Accept-Charset\: ISO-8859-1,utf-8\;q=0.7,*\;q=0.7|0d0a|X-FORWARDED-FOR\: ";\
content: "Via\: ";\
content: "CLIENT-IP\: ";\
content: "Connection\: keep-alive|0d0a|Keep-Alive\: ";\
content: "|0d0a|Cache-Control\: no-cache|0d0a||0d0a|;\
reference:itsoknoproblembro; sid:100000012; rev:1;)
```

kamikaze (with cURL)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 80,443 (msg:"Kamikaze with
Curl GET Flood attack"; flow:established,to_server";\
content: "GET"; offset: 0";\
content: "HTTP/1.1|0d0a|User-Agent\: “; nocase;\
content: “Host\: “;\
content: "Accept\: */*"|0d0a|Accept-Encoding\: deflate|0d0a|X-FORWARDED-FOR\: ";\
content: “Via\: ";\
content: "CLIENT-IP\: ";\
content: "Connection\: keep-alive|0d0a|Keep-Alive\: ";\
reference:itsoknoproblembro; sid:100000013; rev:1;)
```

kamikaze variant (without cURL)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"KAMIKAZE
variant GET Flood"; flow:established,to_server";\
content:"GET"; offset: 0”;\
content:"HTTP/1.1|0d0a|Host: "; \
content:"User-Agent\: ";\
content:"Accept\: */*|0d0a|Accept-Language\:en-us,en\;q=0.5|0d0a|Accept-Encoding\: deflate";\
content:"Accept-Charset\: ISO-8859-1,utf-8\;q=0.7,*\;q=0.7";\
content:"Connection\: Keep-Alive|0d0a|Keep-Alive\: ";\
content: "Cache-Control\: no-cache|0d0a||0d0a|;\
reference:itsoknoproblembro; sid:100000014; rev:1;)
```

kamikaze variant (with cURL)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"KAMIKAZE
variant curl GET Flood";\
flow:established,to_server";\
content:"GET /"; offset: 0";\
content:"User-Agent\: ";\
content:"Host\: ";\
content:"Accept\: */*"|0d0a|Accept-Encoding\: deflate|0d0a|Connection\: keep-alive|0d0a|Keep-
Alive\:300|0d0a||0d0a|";\
reference:itsoknoproblembro; sid:10000015; rev:1;)
```

amos mode

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"AMOS POST
FLOOD attack";\
flow:established,to_server";\
content:"POST"; offset: 0";\
content:"HTTP/1.1|0d0a|Host\: "; \
content:"|0d0a|User-Agent\: Mozilla/4.0 (compatible\; MSIE 6.0\; Windows
NT5.1\;)|0d0a|Content-Length\: 1024|0d0a|Connection\:
Keep-Alive|0d0a|Cache-Control\: no-cache|0d0a|Accept:
*/*|0d0a|Accept-Language\: en-us,en\;q=0.5|0d0a|Accept-Encoding\:
deflate|0d0a|Accept-Charset\: ISO-8859-1,utf-8\;q=0.7,*\;q=0.7|0d0a|TE\:
trailers, deflate|0d0a|Keep-Alive\: 300|0d0a||0d0a|";\
reference:itsoknoproblembro; sid:10000016; rev:1;)
```

Recommended Mitigation: CnC instructions (Snort Rules)

Description: The following rules when implemented create the ability to properly detect if a host within your own network infrastructure has been infected by the ‘itsoknoproblembro’ tools suite. This facilitates the means to properly sanitize possible infected hosts from participating in DDoS attack campaigns.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:”T1 start command
issued for stcurl.php”; flow:established,to_server; content:”stcurl.php?action=start”; nocase;
http_uri; content:”page=“; nocase; reference:itsoknoproblembro-instruction; sid:10000101;
rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:”T1 start command
issued for stcp.php”; flow:established,to_server; content:”stcp.php?action=start”; nocase;
http_uri; content:”page=“; nocase; reference:itsoknoproblembro-instruction; sid:10000102;
rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:”T1 start command
issued for st.indx.php”; flow:established,to_server; content:”indx.php?action=start”; nocase;
http_uri; content:”page=“; nocase; reference:itsoknoproblembro-instruction; sid:10000103;
rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:”T1 start command
issued for stph.php”; flow:established,to_server; content:”stph.php?action=start”; nocase;
http_uri; content:”page=“; nocase; reference:itsoknoproblembro-instruction; sid:10000104;
rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:”T2 brobot
status request”; flow:established,to_server; content:”?action=status”; nocase; http_uri;
reference:itsoknoproblembro-instruction; sid:10000105; rev:1;)

alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:”T1  brobot
status  response”; flow:established,from_server; content:”itsoknoproblembro”; nocase;
reference:itsoknoproblembro-instruction; sid:10000106; rev:1;)

alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:”T1  brobot
status  response”; flow:established,from_server; content:”That is good"; nocase;
reference:itsoknoproblembro-instruction; sid:10000107; rev:1;)
```

Conclusion

Recently, we have seen several of the filenames modified and some of the attacks combined into a single file. From our initial analysis of the update, the signatures have not been modified. We have a comprehensive public threat advisory that will follow this internal report which will focus on the attacks more in depth. Once again we would like to thank the security community for their continued support and efforts.

NOTE: Any findings that correlate with this advisory, please contact PLXsert directly (plxsert@prolexic.com)