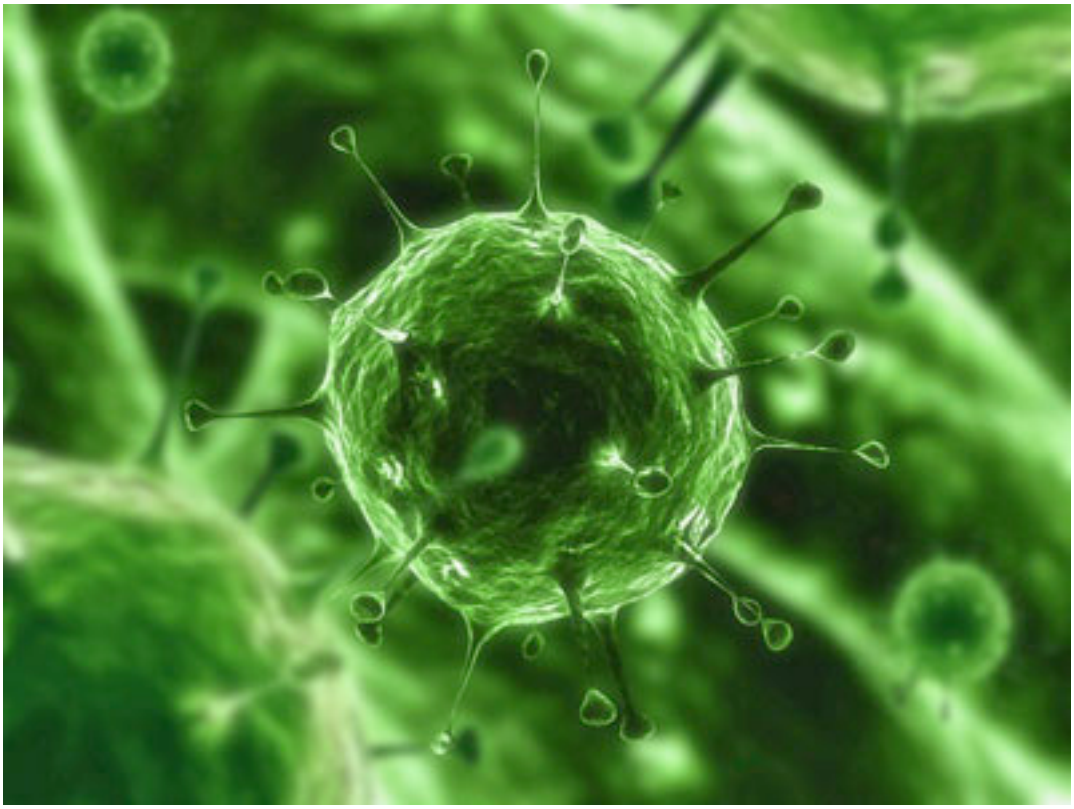
San Diego Exploit Team presents



# **Cha Cha… Choppin down the China Chopper webshell** (say it fast 3*)

## Official malware report

China Chopper CnC | caidao.exe


**Figure 0xFFF: Figured I'd get this out of my system ;)**

| Procedure Summary | |
|---|---|
| **Procedure:** | Malware reverse engineering (dynamic/static analysis) |
| **Author:** | *Rick Flores* |
| **Approved By:** | |
| **Effective Date:** | 08/07/2013 |
| **Source File Location:** | -TBD |

| Revision Summary | | | | |
|---|---|---|---|---|
| **Rev** | **Description of changes** | **Changes by:** | **Review / Approval by:** | **Date** |
| 1.0 | Rough DRAFT | *Flores, Rick* | *N/A* | 08/07/2013 |

| Report Details | | | |
|---|---|---|---|
| **Infected user** | **Computer Name** | **Malware Analyst** | **Date** |
| INFECTED | XEN-00xFFFFF_F.anon.local | *Flores, Rick* | 08/07/2013 |

## Table of Contents


1. Scope ..... 6
2. Investigation goals ..... 7
3. Malware sample analyzed ..... 8
4. Malware variant history, timeline, and special features ..... 8
5. General function and functionality of the malware ..... 13
6. Network behavior (including hosts, domains and ip's accessed) ..... 14
7. Time and local system dependant features ..... 19
8. Snort signature to detetct China Chopper CnC malicious traffic ..... 19
9. References ..... 19

## 1. SCOPE

1.1 Detection Operations created this malware report in an effort to track, categorize, contain, understand root cause and infection vector of said malware sample, user account/s, networked equipment and or computer/s.

## 2. INVESTIGATION GOALS

2.1 Determine extent of infection, uncover actual business risk, data exposure, network weakness, and figure out infection vector and propogation methods.

2.2 More importantly this report should uncover host based indicators that can be used to detect infection, and include network signatures used to alert/prevent potential infection (*McAfee HIPS, Snort, DNS sinkhole*… etc).

## 3. MALWARE SAMPLE ANALYZED

China Chopper CnC | BackDoor.Chopper.1

**Filename** : caidao.exe (the client interface)

**MD5** : md5sum caidao.exe 5001ef50c7e869253a7c152a638eab8a  caidao.exe

**SHA1** : sha1sum caidao.exe 056a60ec1f6a8959bfc43254d97527b003ae5edb  caidao.exe

**SHA256** : be24561427d754c0c150272cab5017d5a2da64d41bec74416b8ae363fb07fd77  caidao.exe

**SSDEEP** : ssdeep,1.1--blocksize:hash:hash,filename

6144:SsTPvGm5RJ5DbeigL9Phruwz1nverLgCBUtePdo:S03GAJ5DbeNZImEP/BUtn,"/root/Desktop/malware/caidao/caidao.exe"

**PACKER USED** : caidao.exe: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed

| | |
|---|---|
| **MD5** | 5001ef50c7e869253a7c152a638eab8a |
| **SHA1** | 056a60ec1f6a8959bfc43254d97527b003ae5edb |
| **SHA256** | be24561427d754c0c150272cab5017d5a2da64d41bec74416b8ae363fb07fd77 |
| **ssdeep** | 6144:SsTPvGm5RJ5DbeigL9Phruwz1nverLgCBUtePdo:S03GAJ5DbeNZImEP/BUtn |
| **File size** | 215.5 KB ( 220672 bytes ) |
| **File type** | Win32 EXE |

**Figure 0x: VirusTotal submission details.**

3.1 Location C:\Documents and Settings**sandb0x**\Local Settings\Temp\caidao.exe

3.2 Moving forward, and for brevity I will be referring to "caidao.exe" simply as the malware sample. When you read `malware sample` or simply 'sample' in the remainder of this report, safely assume I am referring to caidao.exe which is the malicious sample used as the basis of this malware report.

## 4. MALWARE VARIANT HISTORY, TIMELINE, AND SPECIAL FEATURES

4.1 Fisrt publicly documented blog post on the China chopper webshell (Friday, November 16, 2012).

4.2 Fireeye researchers released a part 1 of 2 blog post and new information on the chinese malware (August 7, 2013). Part 1 included a quick surface level analysis of the sample.

4.3 Part 2 promises deeper analysis on its delivery mechanisms, traffic analysis and detection. FireEye also plans to release regular expressions that can be used to find instances of this Web shell.

4.4 Because the strings are not encoded, examining the printable strings in the unpacked binary provides insight into how the backdoor communicates. We were intrigued to see a reference to google.com.hk using the Chinese (simplified) language parameter (Figure 3) as well as references to the text “Chopper” (Figure 4).

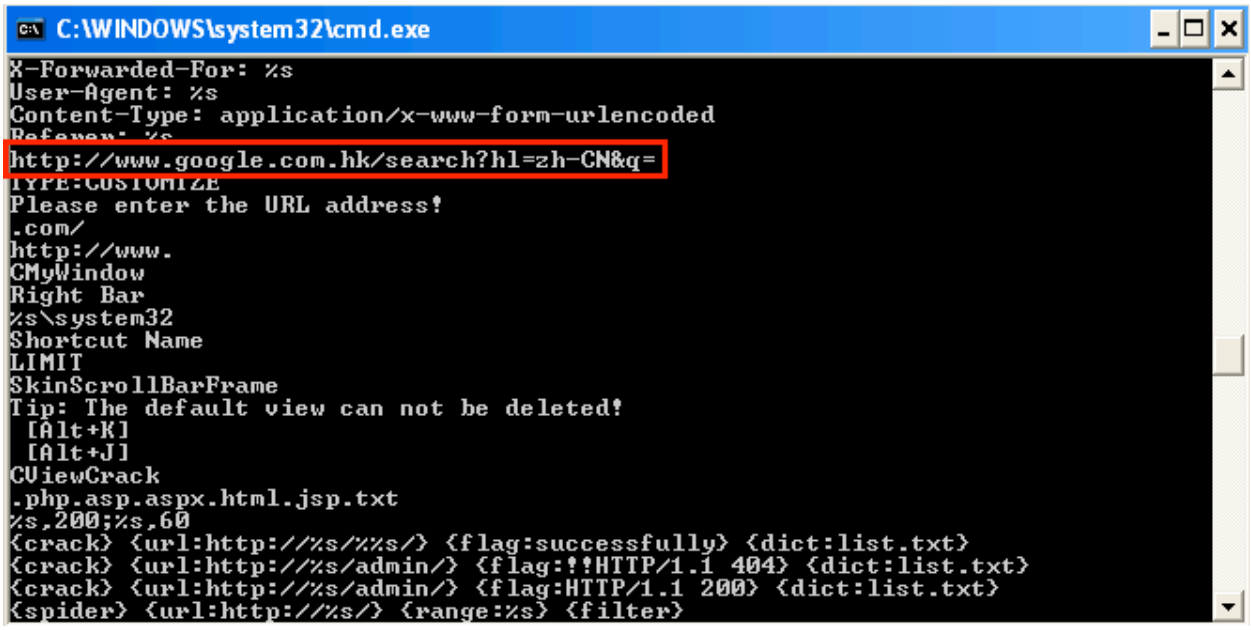



Figure 1: Printable strings refer to www.google.com.hk

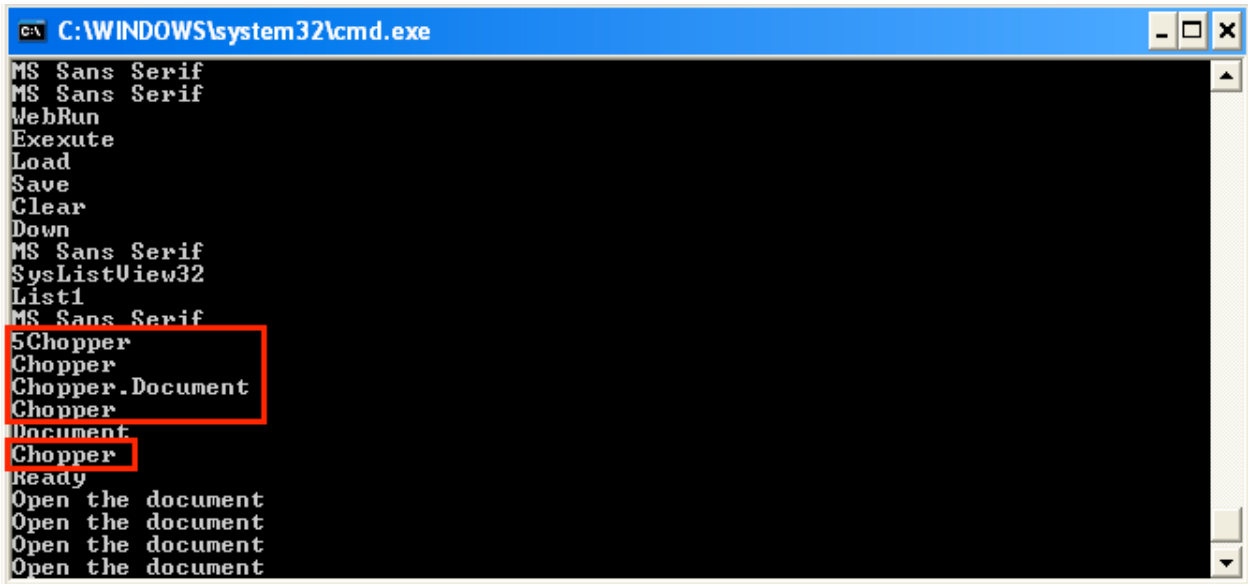



Figure 4: Strings references to the text "Chopper".

## 5. GENERAL FUNCTION AND FUNCTIONALITY OF THE MALWARE

This is a very tiny and feature packed malware sample. It can be used as a RAT, and has several CnC features. Some of the features include:

5.1 Security scanner, spider, password bruteforcer, File Management (File explorer) Database Management (DB client) and Virtual Terminal (Command shell).

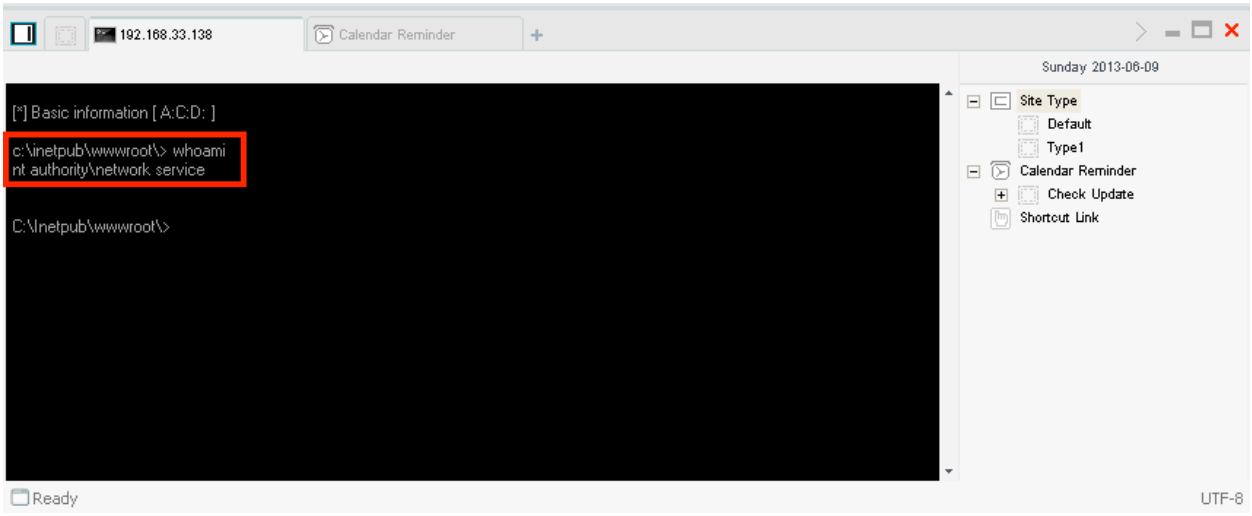



Figure 5: Virtual terminal tabbed (similar to Armitage).

## 6. NETWORK BEHAVIOR (INCLUDING HOSTS, DOMAINS AND IP'S ACCESSED)

6.1 WHOIS can be seen below as having a Beijing, China origin. Domain can be clearly seen as recently updated from this:

```
Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
Domain Name: MAICAIDAO.COM
   Created on: 16-May-09
   Expires on: 16-May-15
   Last Updated on: 30-Jul-11

Registrant:
maicaidao
FangXinYuan
BeiJing
BeiJing, FenTaiQu 100072
China

Administrative Contact:
   caidao, mai  root@maicaidao.com
   maicaidao
   FangXinYuan
   BeiJing
   BeiJing, FenTaiQu 100072
   China
   +86.01086886789

Technical Contact:
   caidao, mai  root@maicaidao.com
   maicaidao
   FangXinYuan
   BeiJing
   BeiJing, FenTaiQu 100072
   China
   +86.01086886789

Domain servers in listed order:
   NS25.DOMAINCONTROL.COM
   NS26.DOMAINCONTROL.COM
```

To this:

Domain Name: MAICAIDAO.COM

Registrar URL: http://www.godaddy.com

Updated Date: 2013-05-04 01:53:31

Creation Date: 2009-05-16 07:17:54

Registrar Expiration Date: 2015-05-16 07:17:54

Registrar: GoDaddy.com, LLC

Registrant Name: mai caidao

Registrant Organization: maicaidao

Registrant Street: FangXinYuan

Registrant Street: BeiJing

Registrant City: BeiJing

Registrant State/Province: FenTaiQu

Registrant Postal Code: 100072

Registrant Country: China

Admin Name: mai caidao

Admin Organization: maicaidao

Admin Street: FangXinYuan

Admin Street: BeiJing

Admin City: BeiJing

Admin State/Province: FenTaiQu

Admin Postal Code: 100072

Admin Country: China

Admin Phone: +86.01086886789

Admin Fax:

Admin Email: root@maicaidao.com

Tech Name: mai caidao

Tech Organization: maicaidao

Tech Street: FangXinYuan

Tech Street: BeiJing

Tech City: BeiJing

Tech State/Province: FenTaiQu

Tech Postal Code: 100072

Tech Country: China

Tech Phone: +86.01086886789

Tech Fax:

Tech Email: root@maicaidao.com

Name Server: NS25.DOMAINCONTROL.COM

Name Server: NS26.DOMAINCONTROL.COM

Name Server: NS31.DOMAINCONTROL.COM

6.2 The malicious POST can be seen below.

```
Hypertext Transfer Protocol
  POST /code.asp HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): POST /code.asp HTTP/1.1\r\n]
      Request Method: POST
      Request URI: /code.asp
      Request Version: HTTP/1.1
    Cache-Control: no-cache\r\n
    X-Forwarded-For: 88.120.198.202\r\n
    Referer: http://172.16.0.10\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
    Host: 172.16.0.10\r\n
```

User-Agent: **User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)**

Host: **172.16.0.10**

Figure 6: User-Agent and malicious host.

6.1 The malicious pages accessed can be seen below.

[+] POST http://www.maicaidao.com/server.asp

[+] POST http://www.maicaidao.com/server.aspx

[+] POST http://www.maicaidao.com/server.php

Figure 7: Different pages accessed.

6.2 The malicious server details can be found below.

GeoIP City/ISP/Organization Results

| IP Address | Country Code | Location | Postal Code | Coordinates | ISP | Organization | Domain | Metro Code |
|---|---|---|---|---|---|---|---|---|
| 184.168.221.27 | US | Scottsdale, Arizona, United States, North America | 85260 | 33.6119, -111.8906 | GoDaddy.com, LLC | GoDaddy.com, LLC | secureserver.net | 753 |

Figure 8: Malicious IP/Host.

## 7. TIME AND LOCAL SYSTEM DEPENDANT FEATURES

7.1 This malware sample requires a valid internet connection, and execution to activate its payload, and send/receive its instructions.

## 8. SNORT SIGNATURE TO DETECT CHOPPER CNC TRAFFIC

Below are examples of rough snort sigs that look for specific Chopper traffic.

1. alert tcp any any -> any 80 ( msg:"China Chopper PHP/Backdoor Detected"; content:"|62 61 73 65 36 34 5f 64 65 63 6f 64 65|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500007; rev:1)

2. alert tcp any any -> any 80 ( msg:"China Chopper PHP/Backdoor Detected"; content: "|63 61 69 64 61 6f 3d|"; content:"|62 61 73 65 36 34 5f 64 65 63 6f 64 65|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500008; rev:1)

3. alert tcp any any -> any any (msg: "China Chopper with first ASPX Payload Command (z1 = cmd shell access) Detected"; flow:to_server,established; content: "FromBase64String"; content: "z1"; content:"POST"; nocase;http_method; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html; classtype:web-application-attack; sid: 900000101;)

4. alert tcp any any -> any any (msg: "China Chopper with *all ASPX Payload Commands (z1 = cmd shell access, & z2 = directory listing/whoami command) Detected"; flow:to_server,established; content: "FromBase64String"; content: "z"; pcre: "/Z\d{1,3}/i"; content:"POST"; nocase;http_method; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html; classtype:web-application-attack; sid: 900000102;)

5. alert tcp any any -> any 80 ( msg:"China Chopper with first ASP Payload Command (z1 = cmd shell access) Detected"; content: "|52 65 73 70 6f 6e 73 65 2e 45 6e 64|"; content:"|49 73 4e 75 6d 65 72 69 63|"; content:"|7a 31|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500066; rev:1)

6. alert tcp any any -> any 80 ( msg:"China Chopper with *all ASP Payload Commands (z1 = cmd shell access, & z2 = directory listing/whoami command) Detected"; content: "|42 52 65 73 70 6f

6e 73 65 2e 45 6e 64|"; content:"|45 6e 63 6f 64 69 6e 67 2e 47 65 74|"; content:"|7a 31|"; content:"|7a 32|";rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500067; rev:1)

| Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|
| 172.16.0.129 | 1300 | 172.16.0.10 | 80 | 6 | China Chopper with first... |
| 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE EXEC atte... |
| 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | GPL ATTACK_RESPONSE ... |
| 192.168.1.102 | 23 | 217.156.93.166 | 61216 | 6 | ET MALWARE Suspicious... |
| 207.35.251.172 | 4031 | 192.168.1.102 | 5920 | 6 | ET SCAN Potential VNC S... |
| 192.168.1.102 | 23 | 217.156.93.166 | 61200 | 6 | GPL TELNET Bad Login |
| 210.114.220.46 | 653 | 192.168.1.102 | 111 | 17 | GPL RPC portmap statu... |
| 207.35.251.172 | 4981 | 192.168.1.102 | 5807 | 6 | ET SCAN Potential VNC S... |
| 207.35.251.172 | 2850 | 192.168.1.102 | 5432 | 6 | ET POLICY Suspicious in... |
| 207.35.251.172 | 3066 | 192.168.1.102 | 1521 | 6 | ET POLICY Suspicious in... |
| 207.35.251.172 | 1134 | 192.168.1.102 | 4333 | 6 | ET POLICY Suspicious in... |
| 207.35.251.172 | 4095 | 192.168.1.102 | 3306 | 6 | ET POLICY Suspicious in... |

☑ Show Packet Data ☑ Show Rule

alert tcp any any -> any 80 ( msg:"China Chopper with first ASP Payload Command (z1 = cmd shell access) Detected"; content: "|52 65 73 70 6f 6e 73 65 2e 45 6e 64|"; content:"|49 73 4e 75 6d 65 72 69 63|"; content:"|7a 31|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500066; rev:1)
/nsm/server_data/securityonion/rules/bug-hunter-eth1-1/local.rules: Line 36

Figure 9: All above sigs have been tested and verified to fire.

RealTime Events | Escalated Events

| .. | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 3 | bug-hunt... | 3.3174 | 2013-08-09 19:16:03 | 192.168.1.90 | 1088 | 184.168.221.27 | 80 | 6 | China Chopper with *all ... |
| RT | 6 | bug-hunt... | 3.3176 | 2013-08-09 19:16:03 | 192.168.1.90 | 1101 | 184.168.221.27 | 80 | 6 | China Chopper PHP/Bac... |
| RT | 42 | bug-hunt... | 3.3183 | 2013-08-09 19:16:25 | 172.16.0.129 | 1334 | 172.16.0.128 | 80 | 6 | China Chopper PHP/Bac... |
| RT | 37 | bug-hunt... | 3.76 | 2013-08-08 17:23:56 | 207.35.251.172 | 2243 | 192.168.1.102 | 21 | 6 | GPL FTP SITE EXEC atte... |
| RT | 1 | bug-hunt... | 3.81 | 2013-08-08 17:23:56 | 192.168.1.102 | 21 | 207.35.251.172 | 2243 | 6 | GPL ATTACK_RESPONSE ... |
| RT | 1 | bug-hunt... | 3.82 | 2013-08-08 17:23:56 | 192.168.1.102 | 23 | 217.156.93.166 | 61216 | 6 | ET MALWARE Suspicious... |
| RT | 4 | bug-hunt... | 3.83 | 2013-08-08 17:23:56 | 207.35.251.172 | 4031 | 192.168.1.102 | 5920 | 6 | ET SCAN Potential VNC S... |
| RT | 2 | bug-hunt... | 3.5 | 2013-08-08 17:23:56 | 192.168.1.102 | 23 | 217.156.93.166 | 61200 | 6 | GPL TELNET Bad Login |
| RT | 1 | bug-hunt... | 3.3 | 2013-08-08 17:23:56 | 210.114.220.46 | 653 | 192.168.1.102 | 111 | 17 | GPL RPC portmap statu... |
| RT | 4 | bug-hunt... | 3.84 | 2013-08-08 17:23:57 | 207.35.251.172 | 4981 | 192.168.1.102 | 5807 | 6 | ET SCAN Potential VNC S... |
| RT | 1 | bug-hunt... | 3.86 | 2013-08-08 17:23:57 | 207.35.251.172 | 2850 | 192.168.1.102 | 5432 | 6 | ET POLICY Suspicious in... |
| RT | 4 | bug-hunt... | 3.89 | 2013-08-08 17:23:58 | 207.35.251.172 | 3066 | 192.168.1.102 | 1521 | 6 | ET POLICY Suspicious in... |

IP Resolution | Agent Status | Snort Statistics | System Ms

Reverse DNS | Enable External DNS

Src IP:

Src Name:

Dst IP:

Show Packet Data | Show Rule

alert tcp any any -> any 80 ( msg:"China Chopper PHP/Backdoor Detected"; content: "|63 61 69 64 61 6f 3d|"; content:"|62 61 73 65 36 34 5f 64 65 63 6f 64 65|"; rawbytes; reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html; classtype:trojan-activity; sid:500008; rev:1)
/nsm/server_data/securityonion/rules/bug-hunter-eth1-1/local.rules: Line 8

**Figure 10: Updated Snort sigs have been tested and verified to fire.**

| Dst IP | DPort | Pr | Event Message |
|---|---|---|---|
| 172.16.0.10 | 80 | 6 | China Chopper with first ASPX Payload Command (z1 = cmd shell access) Detected |
| 192.168.1.102 | 21 | 6 | GPL FTP SITE EXEC attempt |
| 207.35.251.172 | 2243 | 6 | GPL ATTACK_RESPONSE id check returned root |
| 217.156.93.166 | 61216 | 6 | ET MALWARE Suspicious FTP 220 Banner on Local Port (-) |
| 192.168.1.102 | 5920 | 6 | ET SCAN Potential VNC Scan 5900-5920 |
| 217.156.93.166 | 61200 | 6 | GPL TELNET Bad Login |
| 192.168.1.102 | 111 | 17 | GPL RPC portmap status request UDP |
| 192.168.1.102 | 5807 | 6 | ET SCAN Potential VNC Scan 5800-5820 |
| 192.168.1.102 | 5432 | 6 | ET POLICY Suspicious inbound to PostgreSQL port 5432 |
| 192.168.1.102 | 1521 | 6 | ET POLICY Suspicious inbound to Oracle SQL port 1521 |
| 192.168.1.102 | 4333 | 6 | ET POLICY Suspicious inbound to mSQL port 4333 |
| 192.168.1.102 | 3306 | 6 | ET POLICY Suspicious inbound to mySQL port 3306 |

☑ Show Packet Data ☑ Show Rule

```
alert tcp any any -> any 80 ( msg:"China Chopper with first ASPX Payload Command (z1 = cmd shell access) Detected"; content: "|52 65 73 70 6f
6e 73 65 2e 45 6e 64|"; content:"|49 73 4e 75 6d 65 72 69 63|"; content:"|7a 31|"; rawbytes;
reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.ht
ml; classtype:trojan-activity; sid:500027; rev:1)
/nsm/server_data/securityonion/rules/bug-hunter-eth1-1/local.rules: Line 36
```

**Figure 11: Updated Snort sigs have been tested and verified to fire.**

## 9. REFERENCES


1. http://informationonsecurity.blogspot.com/2012/11/china-chopper-webshell.html
2. http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
3. http://www.fireeye.com/blog/technical/botnet-activities-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html
4. https://www.virustotal.com/en/file/be24561427d754c0c150272cab5017d5a2da64d41bec74416b8ae363fb07fd77/analysis/