# blue tangle

blue team dreams, splunk related detections and security insights. I poke around red team and threat actor tools and try to shed some light for cybersecurity wins.

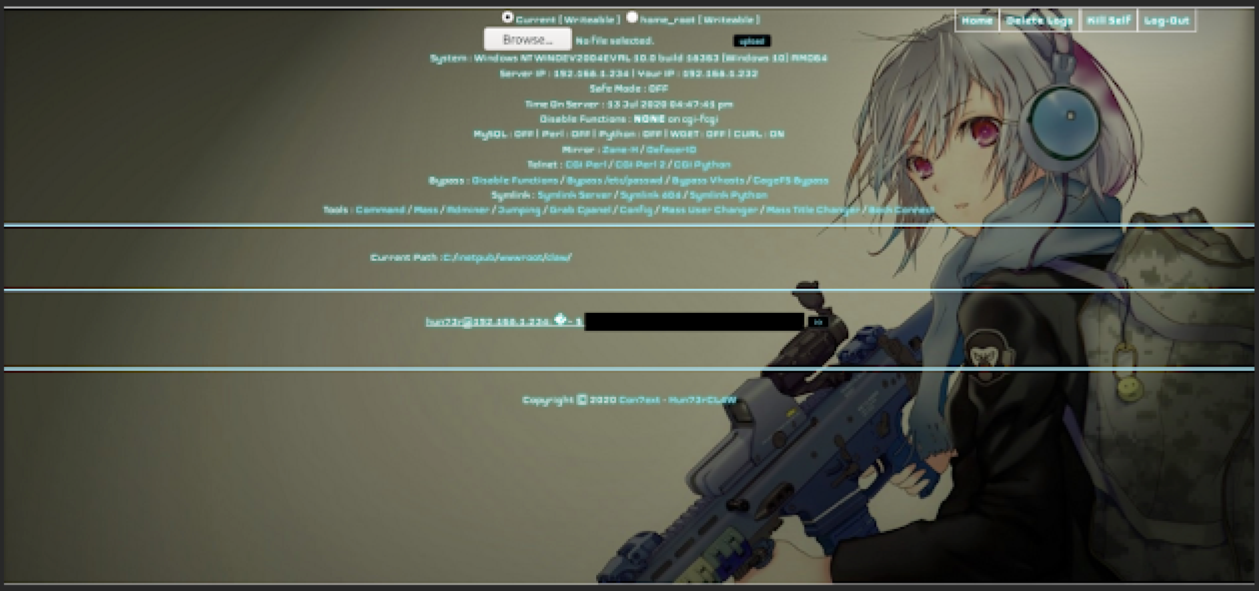
## Webshells automating reconnaissance gives us an easy detection win

- July 22, 2020

For those following along with ATT&CK this entry is about Server Software Component: Web Shell which is now a sub-technique of T1505, specifically it is T1505.003.

If I can avoid combing through web access logs to find stuff like webshells I'll happily dodge it, having looked at the log artefacts left by a number of popular public domain webshells I've found a couple of easy detections based around Windows Event Log (WinEventLog).

We're looking at webshells like "Con7ext", variants of "WSO" and "Alfa Shell":



○ Current [ Writeable ] ○ home_root [ Writeable ]

Browse... No file selected. upload

System : Windows NT WINDEV2004EVAL 10.0 build 18363 [Windows 10] AMD64

Server IP : 192.168.1.234 | Your IP : 192.168.1.232

Safe Mode : OFF

Time On Server : 13 Jul 2020 04:47:41 pm

Disable Functions : NONE on cgi-fcgi

MySQL : OFF | Perl : OFF | Python : OFF | WGET : OFF | CURL : ON

Mirror : Zone-H / DefacerID

Telnet : CGI Perl / CGI Perl 2 / CGI Python

Bypass : Disable Functions / Bypass /etc/passwd / Bypass Vhosts / CageFS Bypass

Symlink : Symlink Server / Symlink 404 / Symlink Python

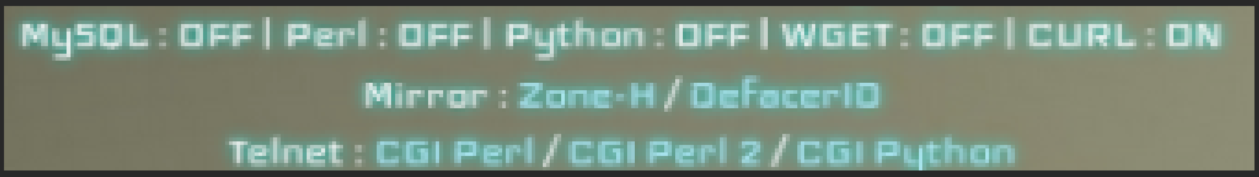
Tools : Command / Mass / Adminer / Jumping / Grab Cpanel / Config / Mass User Changer / Mass Title Changer / Back Connect

Current Path : C:/inetpub/wwwroot/[illegible]/

hun73r@192.168.1.234 ✪ - $

Copyright © 2020 Con7ext - Hun73rCL4W

Specifically we are looking at the parts of the webshell that provide basic reconnaissance as to server components and functionality:

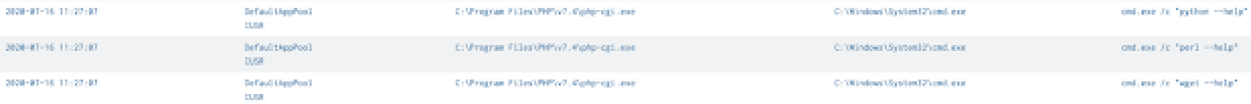


MySQL : OFF | Perl : OFF | Python : OFF | WGET : OFF | CURL : ON

Mirror : Zone-H / DefacerID

Telnet : CGI Perl / CGI Perl 2 / CGI Python

How is the webshell checking if perl, python or wget are installed? In a rather noisy way that we can definitely hunt for:



| | | | | |
|---|---|---|---|---|
| 2020-07-16 11:27:07 | DefaultAppPool<br>IUSR | C:\Program Files\PHP\v7.4\php-cgi.exe | C:\Windows\System32\cmd.exe | cmd.exe /c "python --help" |
| 2020-07-16 11:27:07 | DefaultAppPool<br>IUSR | C:\Program Files\PHP\v7.4\php-cgi.exe | C:\Windows\System32\cmd.exe | cmd.exe /c "perl --help" |
| 2020-07-16 11:27:07 | DefaultAppPool<br>IUSR | C:\Program Files\PHP\v7.4\php-cgi.exe | C:\Windows\System32\cmd.exe | cmd.exe /c "wget --help" |

For IIS and a PHP shell the Splunk SPL to search for this looks something like:

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

```
New_Process_Name=*\cmd.exe AND
(Process_Command_Line="*help*" OR
Process_Command_Line="*-h*")
| table _time Account_Name Creator_Process_Name
New_Process_Name Process_Command_Line
```

So what's going on with this SPL? Let's have a look.

We are looking for the IIS web user (IUSR) and EventCode 4688 (process creation) for cmd.exe processes spawned by php-cgi.exe that include the strings we are looking for ("help" or "-h"). You'll see these three process all spawn within a minute of each other.

The good thing about this detection is that for certain webshells these commands run automatically to populate the informational part of the webshell UI, so traces are left no matter how careful the adversary using the shell is.

Happy hunting!

infosec security splunk web server web shell webshell windows

Popular posts from this blog

### Fastening the Seatbelt on.. Threat Hunting for Seatbelt

- *August 26, 2022*

Quick blog entry on detections for the Ghostpack discovery/reconnaissance tool Seatbelt . This entry will focus on looking at command line parameters that can be caught even if the executable itself is renamed, if I have time we can delve into other event log artefacts another time. From the Seatbelt github repo: …

**READ MORE »**

### Capturing Pcap driver installations

- *June 10, 2020*

Today we're looking at Network Sniffing , ATT&CK technique T1040. This is very much a signature based rule but if you are ingesting WinEventlog:Security (and of course you are, right?) and specifically EventCode 4697 ("A service was installed in the system") then you can take the barebones splunk SPL …

**READ MORE »**

Powered by Blogger

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !