

## ← 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":

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 !

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

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

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

```
index=win10 sourcetype="WinEventLog:Security"  
EventCode=4688 Account_Name=IUSR  
Creator_Process_Name="*\php-cgi.exe"  
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
```

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 !**

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 artefact ...

[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 ...

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 !](#)



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 !](#)