Appendix B

A Hunt Cheat Sheet

This hunt cheat sheet is a resource you can use to look up key information and ideas during your hunts.

Platform

We recommend using the Elastic Stack to store your hunting data (DNS, Sysmon, ETW, etc.). Elastic provides a free SIEM app that enables security operations and threat hunting teams to query, analyze, and visualize their security events quickly, efficiently, and at scale.

Additional resources:

- ☑ *Getting started with the Elastic Stack* (https://ela.st/getting-started)
- ☑ *Elastic SIEM for home and small business blog series* (https://ela.st/siem-for-home)
- ☑ *@Cyb3rWardog's HELK* - an open source hunt platform with advanced analytics capabilities

IPV4 header format (network hunt)

		0	1	2	3
Offsets	Octet	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Octet	Bit	Version IHL	DSCP ECN	Total Length	
0	0	Identification		Flags	Fragment Offset
4	32	Time to Live	Protocol	Header Checksum	
8	64	Source IP Address			
12	96	Destination IP Address			
16	128	Options (If HL>5)			
20	160				
24	192				
28	224				
32	256				

DNS record (network hunt)

Domain Name: google.com

Updated Date: 2015-06-12...

Creation Date: 1997-09-15...

Ref: elastic.co, whois, docs.microsoft.com

Sysmon event (host hunt)

Event ID	
1	Process creation - provides extended information about a newly created process
2	A process changed a file creation time - file creation time is modified by process
3	Network connection - logs TCP/UDP connections on the machine
4	Sysmon service state changed - state of the Sysmon service (started or stopped)
5	Process terminated -reports when a process terminates
6	Driver loaded - driver being loaded on the system
7	Image loaded - logs when a module is loaded in a specific process
8	CreateRemoteThread - a process creates a thread in another process
9	RawAccessRead - detects reading operations from the drive using the \\.\
10	ProcessAccess - reports when a process opens another process
11	FileCreate - file is created or overwritten
12	RegistryEvent (Object create and delete) - registry key/value create and delete
13	RegistryEvent (Value Set) - registry value modifications
14	RegistryEvent (Key and Value Rename) - registry key/value rename operations
15	FileCreateStreamHash - file stream is created
16	n/a - Sysmon configuration change (cannot be filtered)
17	PipeEvent - Named pipe created
18	PipeEvent - Named pipe connected
19	WmiEventFilter activity - logs when a WMI event filter is registered
20	WmiEventConsumer activity - logs the registration of WMI consumers
21	WmiEventConsumerToFilter activity - logs when a WMI consumer binds to a filter
22	DNSEvent - logs when a process executes a DNS query
255	Error

Analysis Techniques

IOC matching

We are not recommending IOC matching, but are discussing it here for the sake of completeness. Matching involves using IOCs to detect malicious activity. These can be file attributes (hashes, filenames, import hashes), network artifacts (domains, IP addresses), registry keys (key values, key sources), and known compromised user accounts and machines. This is a weak approach, because indicators have short life spans and should be automated as soon as time and resources permit.

Frequency and outlier analysis

Frequency and counts of artifacts help discover anomalies. Anomalies do not necessarily represent suspicious activity, but when used correctly they provide leads for investigation. For example, DNS request counts show the occurrences of a registry key, or the least occurring scheduled tasks and WMI objects in the environment.

Comparative analysis

Comparative analysis uses a gold or baseline image to find deltas. The gold image is the clean slate prior to any user interaction. You can compare workstations to the baseline image. This is especially important if your users are unable to install new software or don't commonly do so. Any deviation from that baseline gold image might be an anomaly worth investigating.

Temporal proximity

Using time can be very powerful because it relates to network and event data. For instance, small packets being sent on a routine time interval may indicate malware beaconing or show Windows events in a sequential order. This can illuminate malicious activity through executions like process create, process execute, DNS request, network connection, process terminate, and file delete.

Data enrichment

Public data sources and threat intel feeds are immensely powerful for data enrichment. For instance, you can search file attributes in VirusTotal and search network artifacts in WHOIS databases and tools like Domain Tools or Central Ops.

Quick Wins

How do you detect persistence techniques?

Ref: sysinternals/downloads/autoruns

- ☑ Look for files set to run automatically
- ☑ Pay close attention to outliers

What forensics data should you look for?

Ref: powerforensVics.readthedocs.io

- ☑ Check the Prefetch and Shimcache
- ☑ Get-ForensicPrefetch: file execution forensics
- ☑ Get-ForensicShimcache: AppCompatCache forensics

How do you look for evasion techniques?

Malware files may be named to pose as native Windows files. Compare filenames within %system% to files on disk. Be suspicious when a name matches but the file path does not.

How do you look for injected code?

Look for remote thread creation (e.g. Sysmon thread injection detection), for example:

<CreateRemoteThread onmatch=”include”>

<TargetImage condition=”image”>lsass.exe</TargetImage>

</CreateRemoteThread >

Are your files trusted?

Ref: sysinternals/downloads/sigcheck

Examine certificate information by looking for untrusted processes. Enrich your findings by looking specifically for:

- ☑ Persistent untrusted files
- ☑ Running untrusted processes
- ☑ Running untrusted processes generating network traffic (e.g., netstat)

How do I find credential theft, like KERBEROAST?

Ref: adsecurity.org

- ☑ Frequency of Eventid 4769 - A Kerberos service ticket was requested
- ☑ Alert for KerberosRequestorSecurityToken
- ☑ Search for use of invalid accounts

What file properties are interesting?

Ref: msdn.microsoft.com

- ☑ Examine signer/certificate information
- ☑ Don’t trust the file name on disk – compare it to FileVersion Info.OriginalFilename
- ☑ Look for files running out of %temp% or %downloads%

Is this an administrator?

Living off the land techniques use legitimate tools. Monitor PowerShell, WMI, InstallUtil, MSBUILD, RegAsm, and other tools that allow code execution.

What is the IDS rule syntax? [Network searching help]

Ref: Snort Manual

alert tcp any any -> 192.168.1.0/24 111 (content: "|00 01 86 a6|"; msg: "mountd access";)

WHAT IS THE YARA RULE SYNTAX [FILE SEARCHING HELP]

What is the YARA rule syntax? [File searching help]

Ref: yara.readthedocs.io

rule Example { strings: $string = { } condition: $string }

What is the EQL syntax?

EQL is a language that can match events, generate sequences, stack data, build aggregations, and perform analysis

Ref: https://eql.readthedocs.io/

process where process_name == "svchost.exe" and command_line != "* -k *"

The Elastic Guide to Threat Hunting

Learn how to stop targeted attacks before damage and loss with step-by-step instructions and practical advice on how to hunt.

About the Authors

Brent Murphy is a Security Research Engineer II at Elastic where he creates behavioral detections for emerging threats. He previously served on the advanced threat team at a F500 financial institution where he co-developed a threat hunting program.

David French is a Security Research Engineer II at Elastic, focusing on analyzing adversary behavior and developing detections. He formerly led threat hunting strategy and incident response at a large financial institution.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-12-6