

Zero day Forensics

HOW TO ANALYZE NEW EXPLOITS

Zero Day

About the Speaker

2

- ▶ 20 books (Including 3 on forensics, 5 on computer security, 1 on cryptology)
- ▶ Over 40 industry certifications including several forensic certifications
- ▶ Member and Diplomat of the American College of Forensic Examiners
- ▶ Chair of the cyber forensics board for the American College of forensic Examiners
- ▶ 2 Masters degrees and multiple graduate certificates
- ▶ 7 Computer science related patents
- ▶ Over 25 years experience, over 15 years teaching/training
- ▶ Helped create CompTIA Security+, Linux+, Server+. Helped revise CEH v8
- ▶ Frequent consultant/expert witness
- ▶ Presents workshops talks at security conferences all over the world including Defcon, Hakon India, Hakon Africa, ADFSL, ISC2 Security Congress, Secure World, etc.

www.chuckeasttom.com

chuck@chuckeasttom.com

Zero Day

Finding them

3

- ▶ Since these are new and unknown there are no signatures for them. So traditional search mechanisms will not work.

Zero Day

Finding them

While motives range from ethical to malicious, the end goal is the same: discover vulnerabilities that expose risk. As figure 1 illustrates, the vulnerability research lifecycle is a process that starts with identifying the software vulnerability through static analysis, fuzzing, etc, establishing a 'proof of concept' (PoC) to demonstrate the existence of exploitability, then disclosure to the vendor, and subsequently the public. When a proven vulnerability (proven by existence of PoC or other exploit code) is released to (or used in) the public without prior vendor engagement, it is referred to as a 0day.

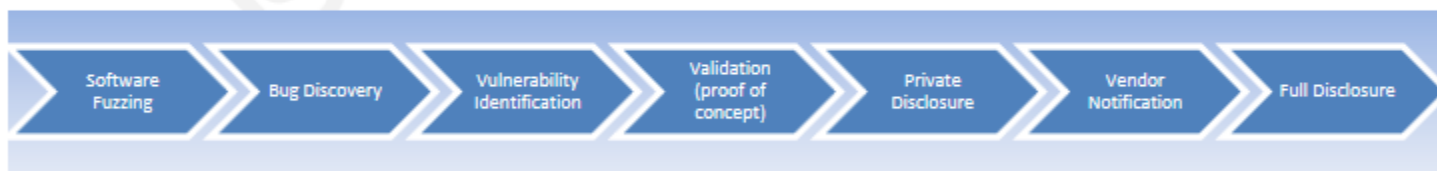


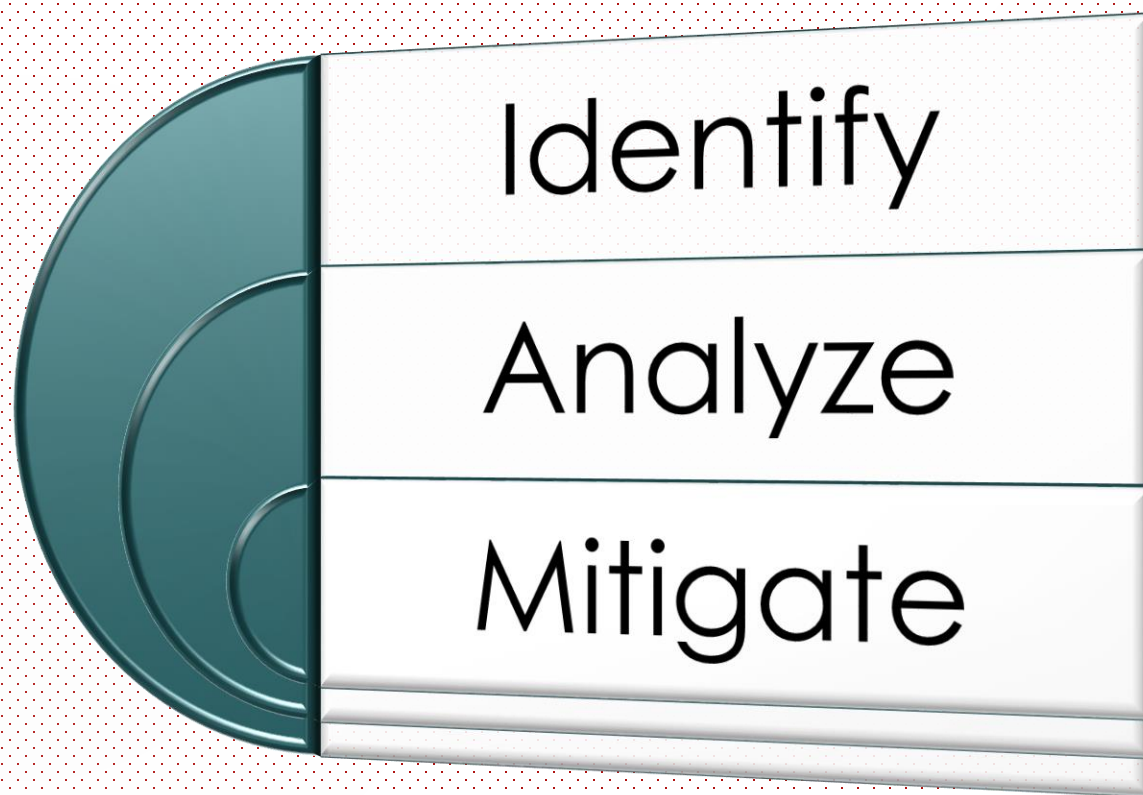
Figure 1: Vulnerability Research Lifecycle

<https://www.sans.org/reading-room/whitepapers/incident/responding-zero-day-threats-33709>

Zero Day

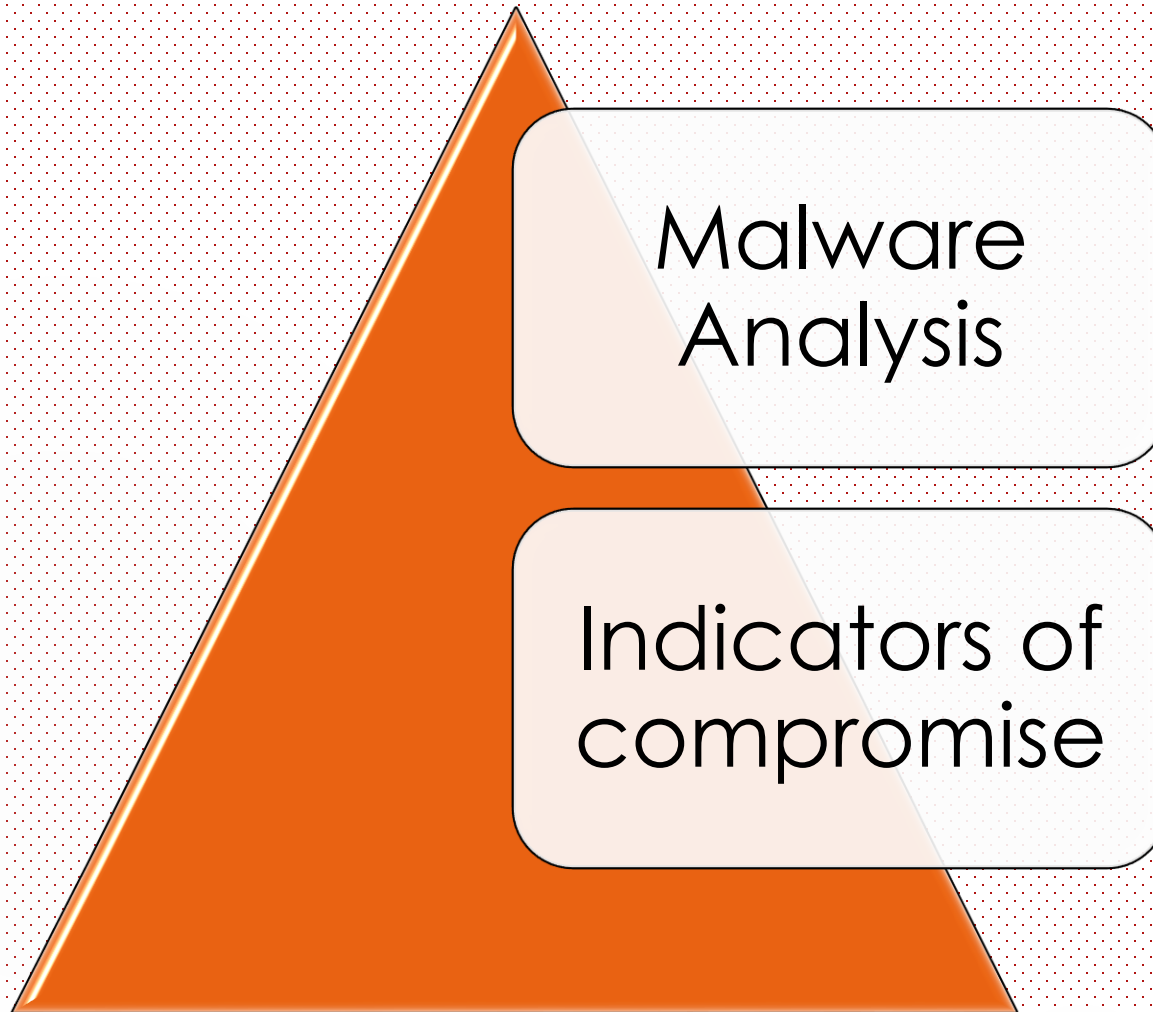
Zero Day Incident Response

5



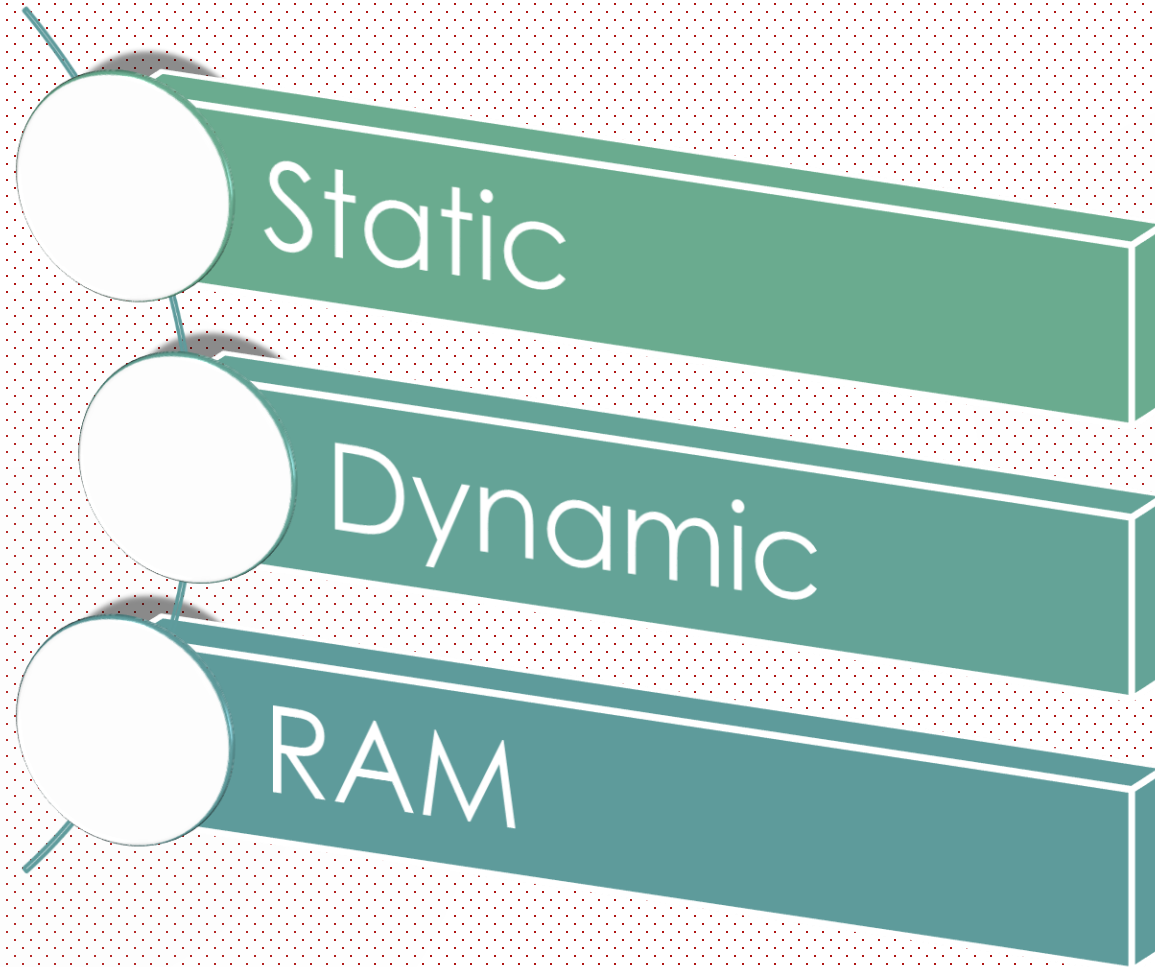
Zero Day

Methods



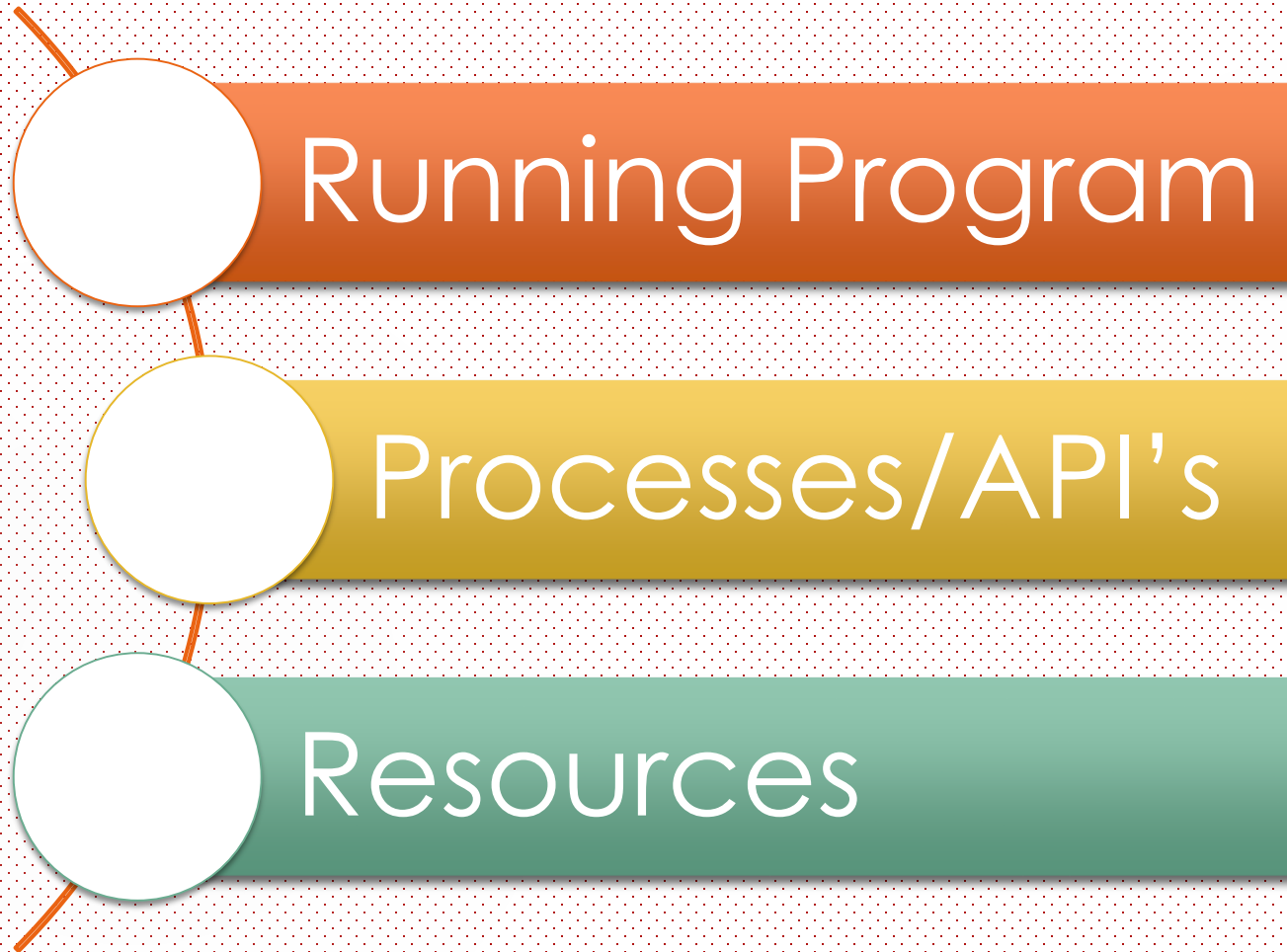
Zero Day

Malware Analysis



Zero Day

Dynamic Analysis



Zero Day

Capture Memory

- Dumpit
- FTK Imager
- OSForensics
- RAM Capture

Zero Day

Analyzing RAM

- ▶ Regardless of how you capture the memory, memory is usually analyzed using volatility.
- ▶ <http://www.volatilityfoundation.org/releases>

Indicators of Compromise

11

Network, file, or operating system artifact that has a high chance of indicating an attack or breach.

Anti malware analyzes IoC such as virus signatures, MD5 hashes of malware files or URLs or domain names of botnet command and control servers.

However, with a zero-day your anti malware won't see any of these.

Zero Day

Windows Service Startup Order

12

Session Manager Subsystem (SMSS) first marks itself, and its main thread as critical objects. (note you will see more than one SMSS)

SMSS starts both Wininit and the CSRSS Client/Server Runtime Subsystem

Then Wininit starts services.exe

Services.exe starts all the other services. Expect to see many svchost.exe

Svchost.exe is a process on your computer that hosts, or contains, other individual services that Windows uses to perform various functions. For example, Windows Defender uses a service that is hosted by a svchost.exe process.

Zero Day

Indicators of Compromise

13

In Windows you can find newly installed system components

Open a command window and navigate to [\\Windows\System32](#)
run *dir /o:d*

```
05/03/2016 11:26 PM          623,112 igfxDH.dll
05/03/2016 11:26 PM    1,259,496 IntelWiDiSecureSourceFilter32.dll
05/03/2016 11:26 PM    597,480 IntelWiDiMux32.dll
05/03/2016 11:26 PM     97,800 igfxCUIServicePS.dll
05/03/2016 11:26 PM    292,832 igfxCUIService.exe
05/03/2016 11:26 PM    250,376 igfxCPL.cpl
05/03/2016 11:26 PM    1,775,624 igfxcmjit32.dll
05/03/2016 11:26 PM    172,552 igfx11cmrt32.dll
05/03/2016 11:26 PM    135,144 IntelWiDiMCUMD32.dll
05/03/2016 11:26 PM    103,400 IntelWiDiLogServer32.dll
05/03/2016 11:26 PM    1,803,784 igdrcl32.dll
05/03/2016 11:26 PM    200,200 igdde32.dll
05/03/2016 11:26 PM    338,952 igdbcl32.dll
05/03/2016 11:26 PM    161,288 igdail32.dll
05/03/2016 11:26 PM    6,518,792 ig7icd32.dll
05/03/2016 11:26 PM    4,402,144 Gfxv4_0.exe
05/03/2016 11:26 PM    4,398,552 Gfxv2_0.exe
05/03/2016 11:26 PM     935,392 GfxUIEx.exe
05/03/2016 11:26 PM     77,832 OpenCL.DLL
05/03/2016 11:26 PM     565,216 DPTopologyApp.exe
05/03/2016 11:26 PM     176,648 igfxCoIn_v4358.dll
05/03/2016 11:26 PM    2,179,872 IntelWiDiVAD32.exe
05/03/2016 11:26 PM     626,696 MetroIntelGenericUIFramework.dll
05/03/2016 11:26 PM     111,624 IccLibDll.dll
05/03/2016 11:26 PM    17,854,984 igdfcl32.dll
```

Indicators of Compromise

14

Look for files that are named closely to system files. For example:

`nvsvc32.exe` or `serv1ces.exe` in the `system32` folder.

Zero Day

Indicators of Compromise

15

Malware is often set to start automatically. Look in the following registry keys for malware that has been added to the startup

`\Software\Microsoft\Windows\CurrentVersion\Run`

`\Software\Microsoft\Windows\CurrentVersion\RunOnce`

`\Software\Microsoft\Windows\CurrentVersion\RunOnceEx`

`\Software\Microsoft\Windows\CurrentVersion\RunServices`

`\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`

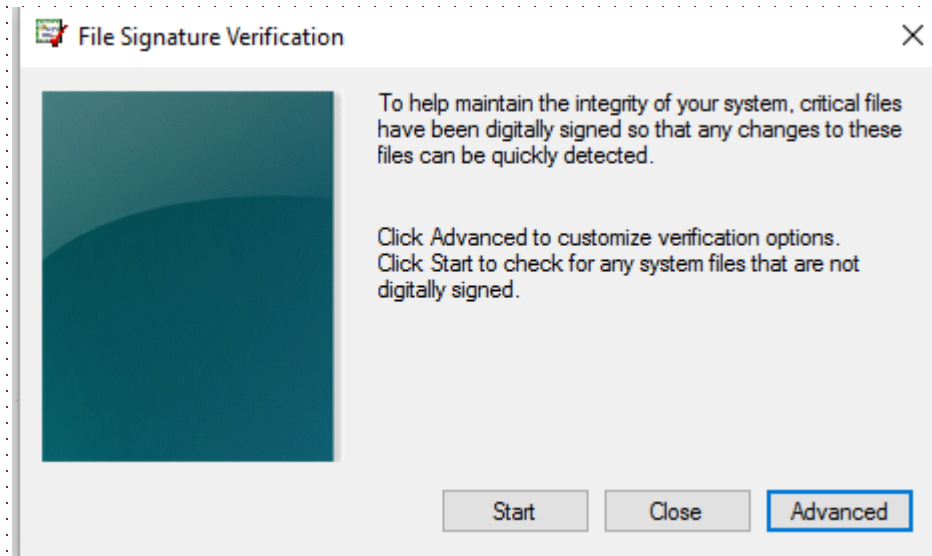
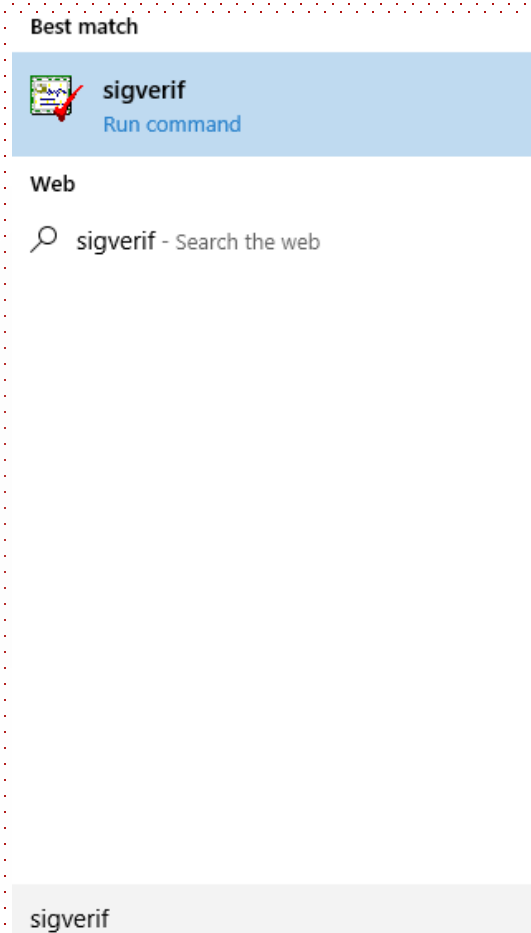
`\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon`

Zero Day

Indicators of Compromise

16

Microsoft Windows has a utility to verify the signatures of system files.



Zero Day

15 top IoC

1. Unusual outbound network traffic
2. Anomalies in Privileged User Account Activity
3. Geographical Irregularities
4. Other Log-in Red Flags
5. Swells in Database Read Volume
6. HTML Response Sizes
7. Large Numbers of Requests for the Same File
8. Mismatched Port-Application Traffic
9. Suspicious Registry or System File Changes
10. DNS Request Anomalies
11. Unexpected Patching
12. Mobile Device Profile Changes
13. Data in the Wrong Places
14. Web traffic with non-human behavior
15. Signs of DDoS.

-<http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?>

Zero Day

Rootkitrevealer - Sysinternals

- ▶ A Free download and part of sys internals
- ▶ <https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>
- ▶ Rootkitrevealer will not clean the machine, it does, however, scan the hard drive and the registry for possibly problematic files / entries.
- ▶ These are then highlighted for the user to take action, if required.

Zero Day

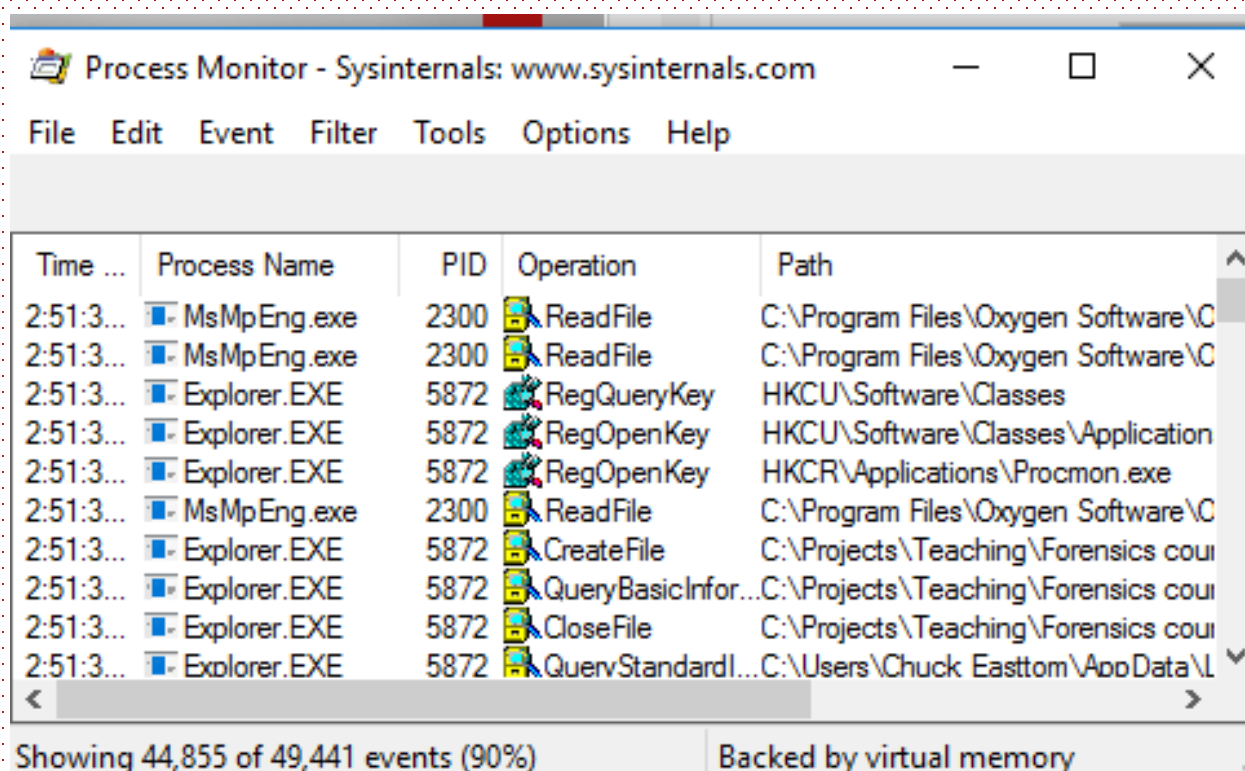
Process Explorer - Sysinternals

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	93.11	0 K	8 K	0		
System	0.46	40 K	648 K	4		
Interrupts	0.34	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		224 K	612 K	416		
Memory Compression	< 0.01	724 K	173,848 K	3368		
csrss.exe	< 0.01	1,132 K	3,012 K	548		
csrss.exe	0.04	1,152 K	5,152 K	644		
wininit.exe		764 K	2,712 K	668		
services.exe	0.49	2,900 K	5,212 K	780		
svchost.exe	< 0.01	6,820 K	17,128 K	892	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		888 K	4,732 K	4236		
WmiPrvSE.exe		6,492 K	11,736 K	4432		
dllhost.exe		3,288 K	6,796 K	2664		
WmiPrvSE.exe		2,864 K	9,700 K	2172		
dllhost.exe		2,268 K	9,348 K	6444	COM Surrogate	Microsoft Corporation
ShellExperienceHost...	Susp...	48,492 K	40,104 K	8184	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		36,388 K	36,244 K	2484	Runtime Broker	Microsoft Corporation
unsecapp.exe		1,108 K	6,140 K	9556	Sink to receive asynchronou...	Microsoft Corporation
SystemSettingsBroker...		3,480 K	14,188 K	4256	System Settings Broker	Microsoft Corporation
SkypeHost.exe	Susp...	4,880 K	212 K	2796	Microsoft Skype Preview	Microsoft Corporation
SearchUI.exe	Susp...	71,208 K	55,892 K	8968	Search and Cortana applicati...	Microsoft Corporation
ApplicationFrameHost...		3,084 K	13,900 K	9472	Application Frame Host	Microsoft Corporation
smartscreen.exe		6,796 K	10,176 K	8768	SmartScreen	Microsoft Corporation
svchost.exe	0.02	6,028 K	10,368 K	960	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	30,756 K	47,468 K	1096	Host Process for Windows S...	Microsoft Corporation
sihost.exe		5,688 K	17,768 K	5492	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		7,932 K	16,116 K	3468	Host Process for Windows T...	Microsoft Corporation
taskhostw.exe		6,572 K	15,636 K	10128		
svchost.exe		16,992 K	18,064 K	1168	Host Process for Windows S...	Microsoft Corporation

CPU Usage: 6.89% Commit Charge: 85.46% Processes: 111 Physical Usage: 80.67%

Day

Process Monitor - Sysinternals



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
2:51:3...	MsMpEng.exe	2300	ReadFile	C:\Program Files\Oxygen Software\C
2:51:3...	MsMpEng.exe	2300	ReadFile	C:\Program Files\Oxygen Software\C
2:51:3...	Explorer.EXE	5872	RegQueryKey	HKCU\Software\Classes
2:51:3...	Explorer.EXE	5872	RegOpenKey	HKCU\Software\Classes\Application
2:51:3...	Explorer.EXE	5872	RegOpenKey	HKCR\Applications\Procmon.exe
2:51:3...	MsMpEng.exe	2300	ReadFile	C:\Program Files\Oxygen Software\C
2:51:3...	Explorer.EXE	5872	CreateFile	C:\Projects\Teaching\Forensics cou
2:51:3...	Explorer.EXE	5872	QueryBasicInfor...	C:\Projects\Teaching\Forensics cou
2:51:3...	Explorer.EXE	5872	CloseFile	C:\Projects\Teaching\Forensics cou
2:51:3...	Explorer.EXE	5872	QueryStandardI...	C:\Users\Chuck Easttom\AppData\L

Showing 44,855 of 49,441 events (90%) Backed by virtual memory

Zero Day

Questions

www.chuckeasttom.com
chuck@chuckeasttom.com

Zero Day