Zero day Forensics

HOW TO ANALYZE NEW EXPLOITS

Zero Day

About the Speaker

- 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

Finding them

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

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.

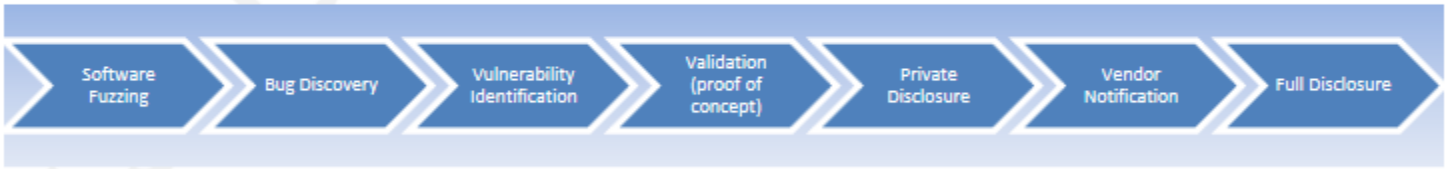
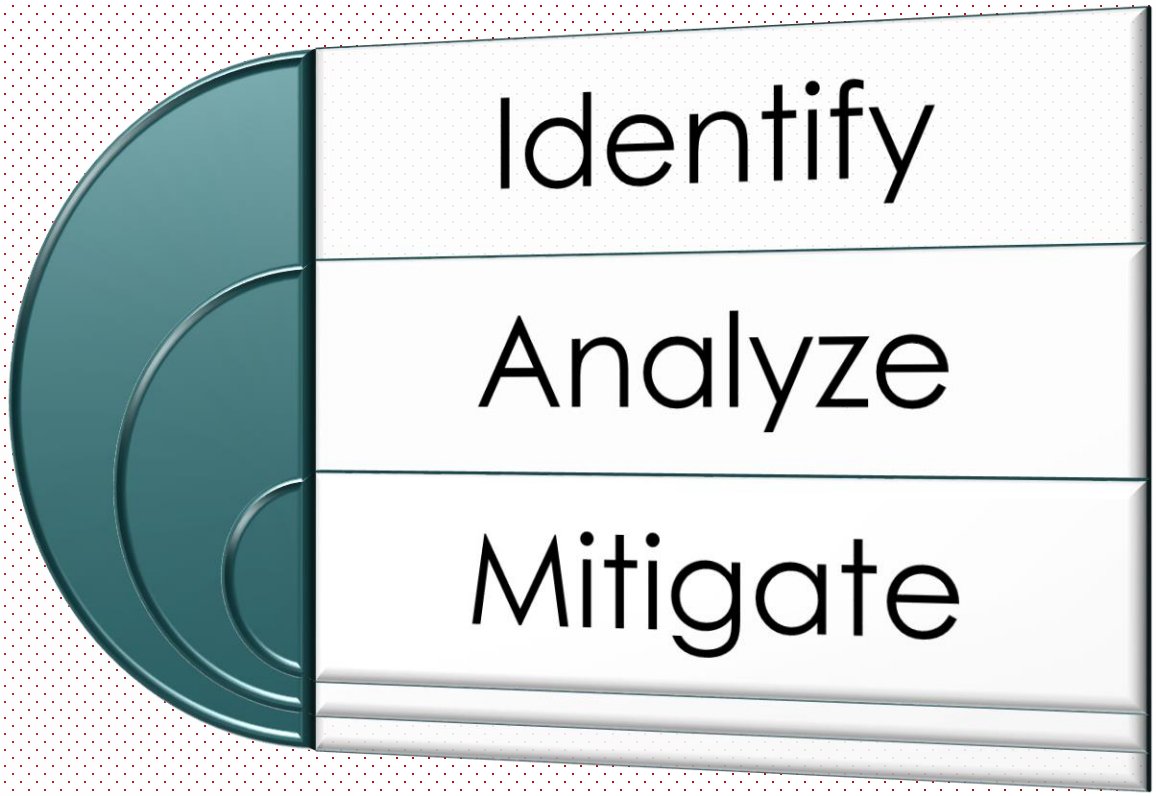


Figure 1: Vulnerability Research Lifecycle

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

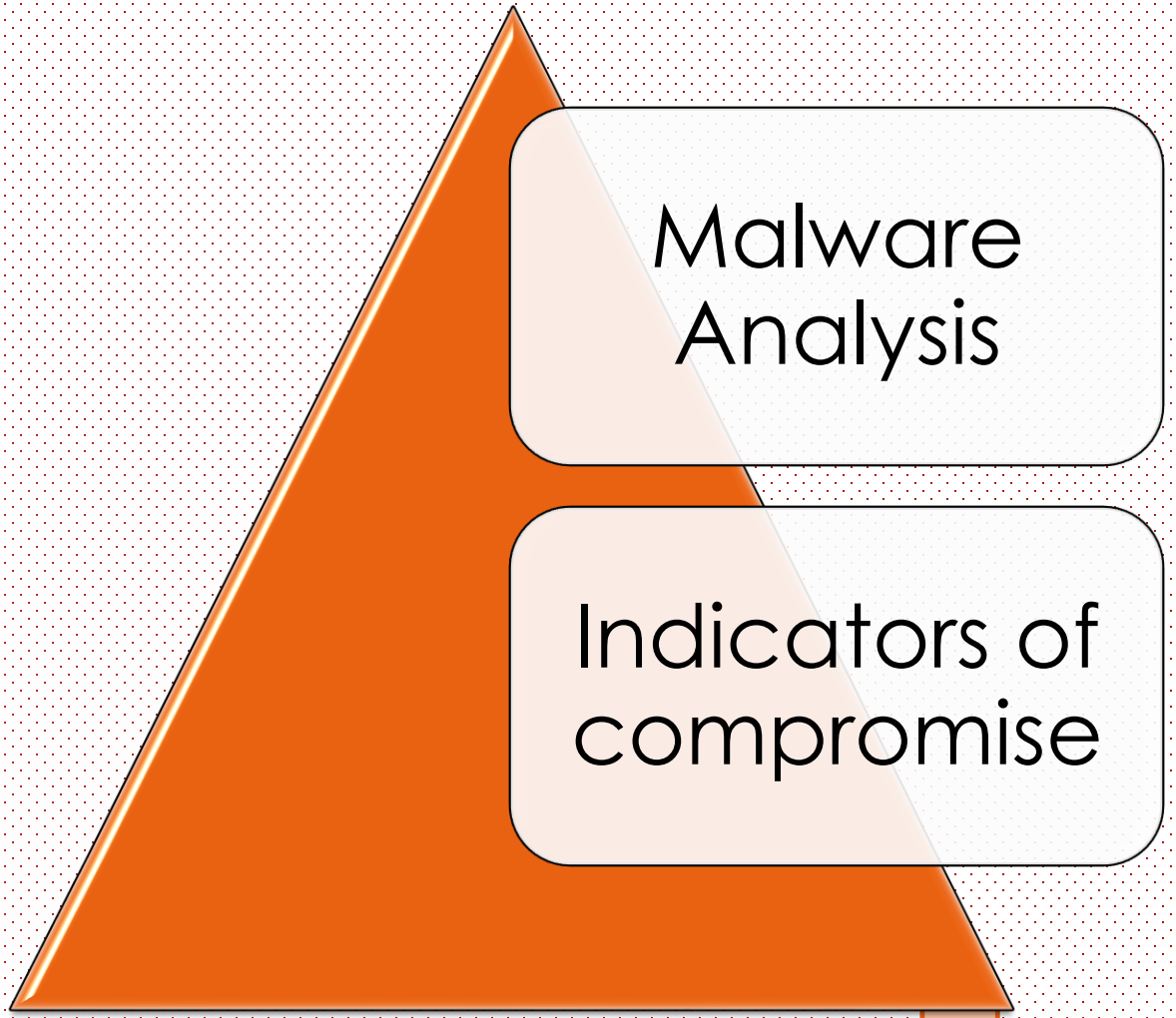
Zero Day

Zero Day Incident Response



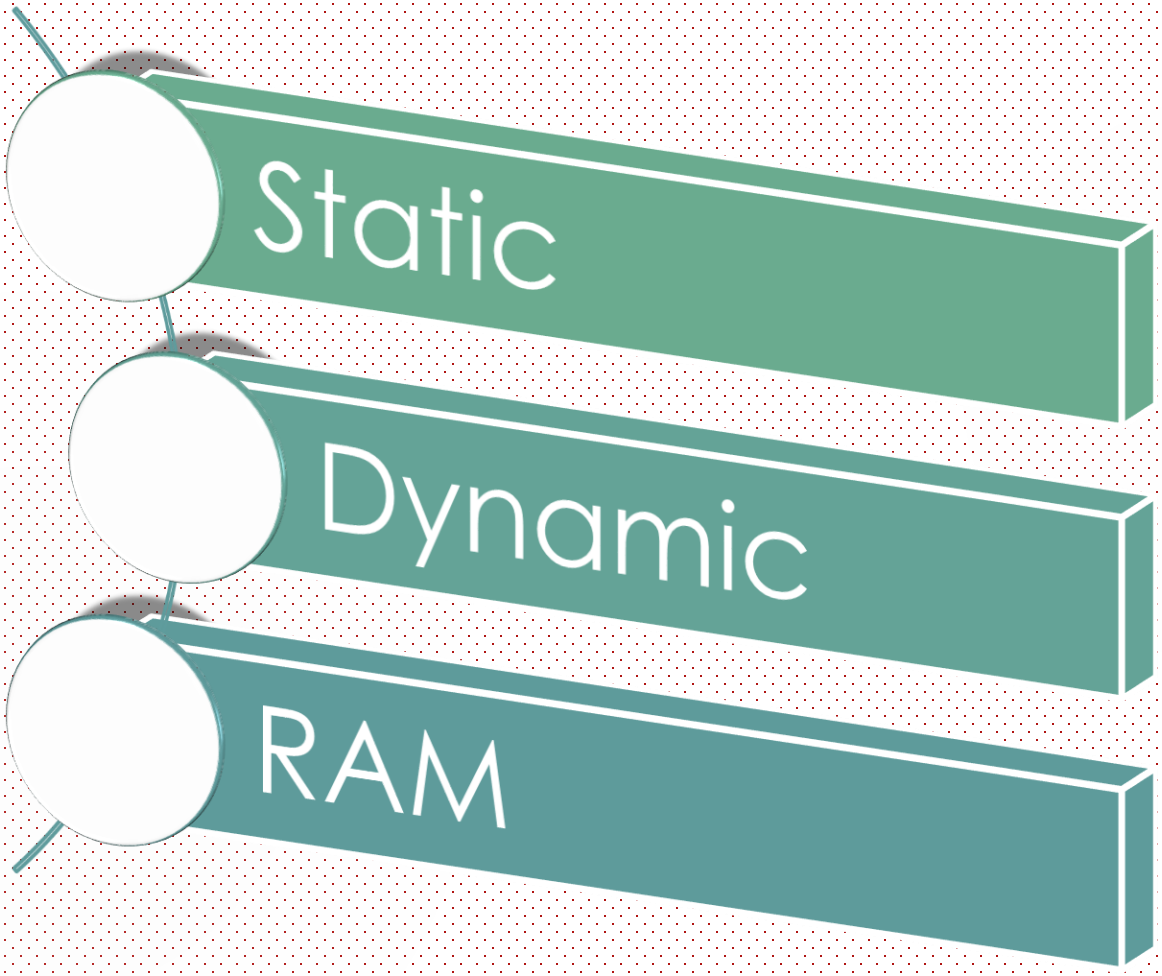
Zero Day

Methods

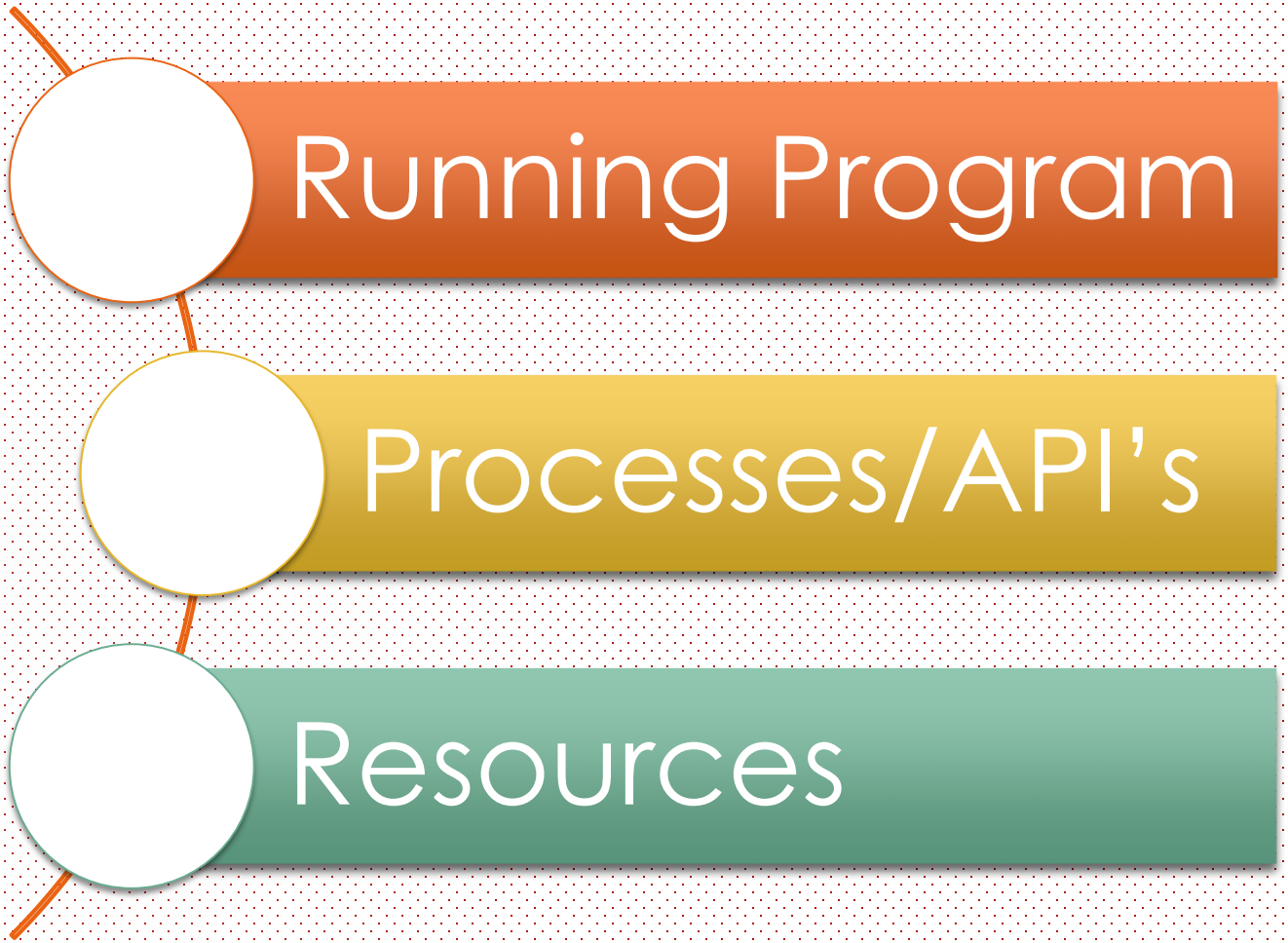


Zero Day

Malware Analysis



Dynamic Analysis



Zero Day

Capture Memory

- Dumpit
- FTK Imager
- OSForensics
- RAM Capture

Analyzing RAM

- Regardless of how you capture the memory, memory is usually analyzed using volatility.

- http://www.volatilityfoundation.org/releases

Indicators of Compromise

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

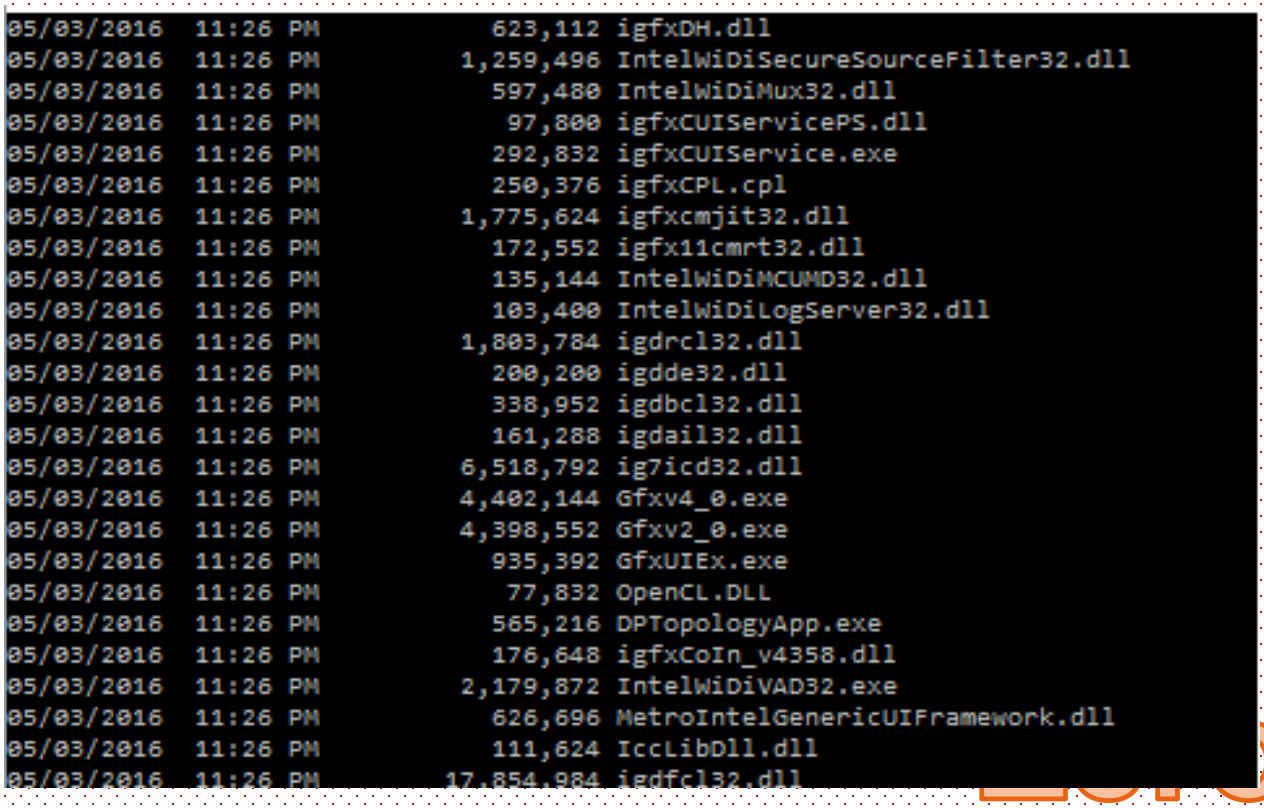
Session Manager Subsystem (SMSS) first marks itself, and its main thread as critical objects. (note you will see more than one SMSS)
SMSS starts both Wininit and the CSRSS Client/Server Runtime Subsystem
Then Winnit stars services.exe
Services.exe starts all the other services. Expect to see many svchost.exe

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.

Indicators of Compromise

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
```

Zero Day

Indicators of Compromise

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

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

Indicators of Compromise

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

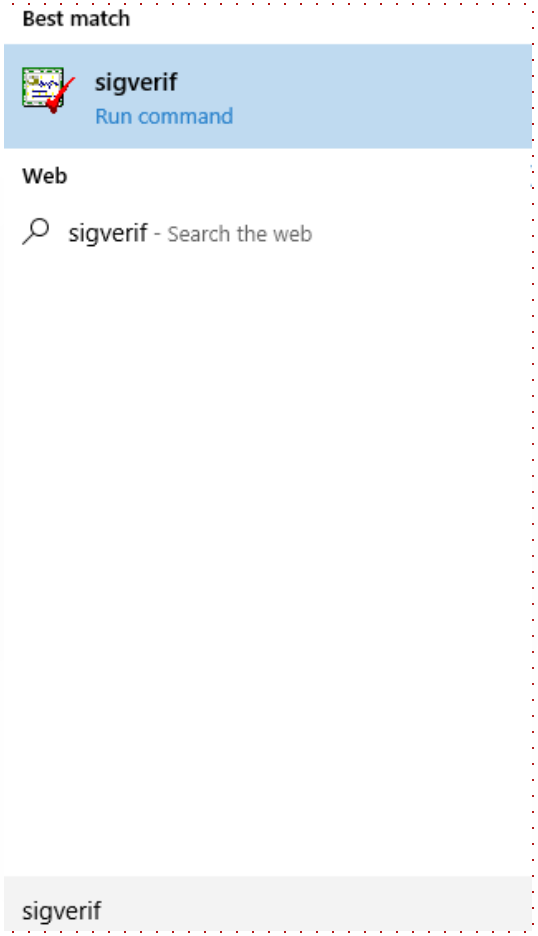
\Software\Microsoft\Windows\CurrentVersion\RunServices

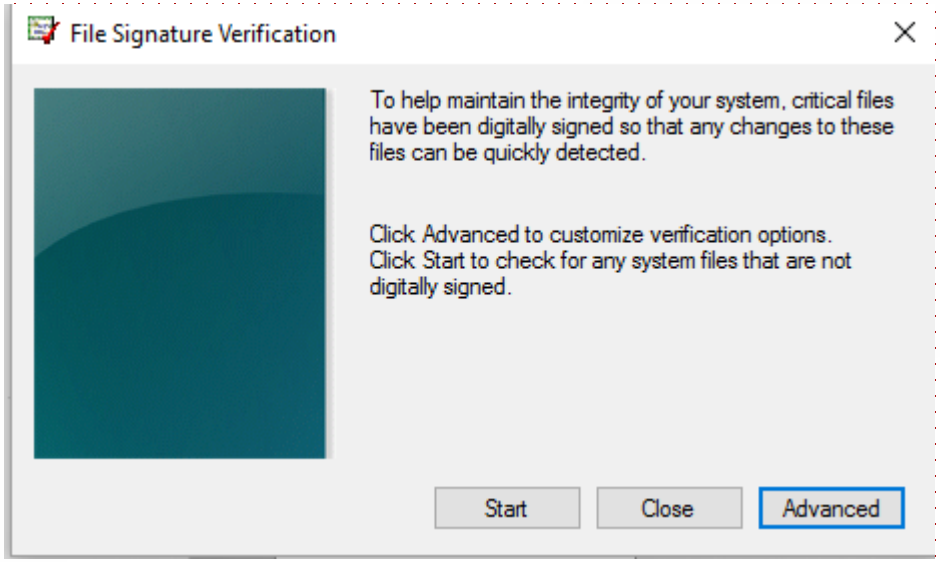
\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Indicators of Compromise

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?

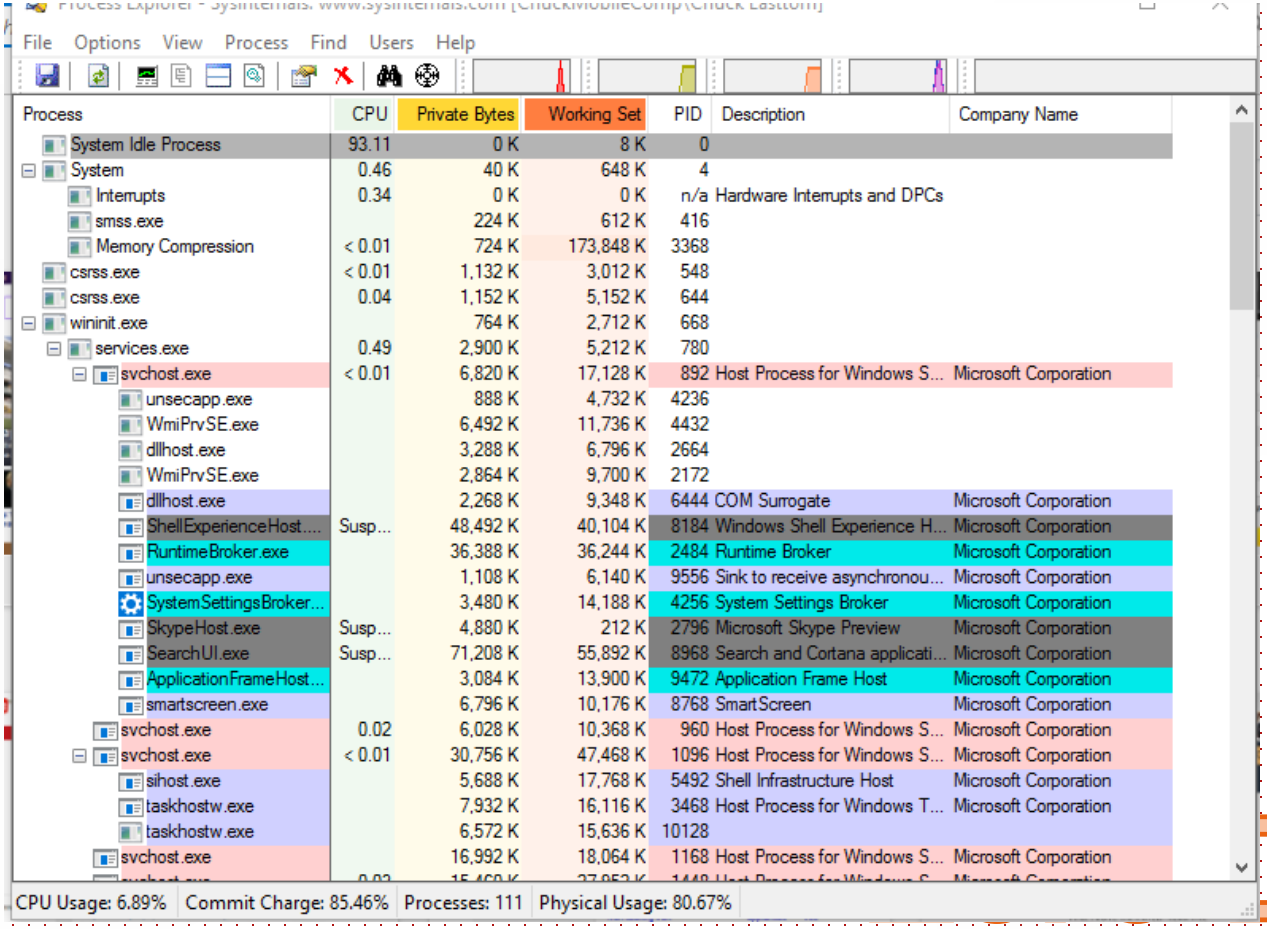
Rootkitrevealer - Sysinternals

- A Free download and part of sys internals
- https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

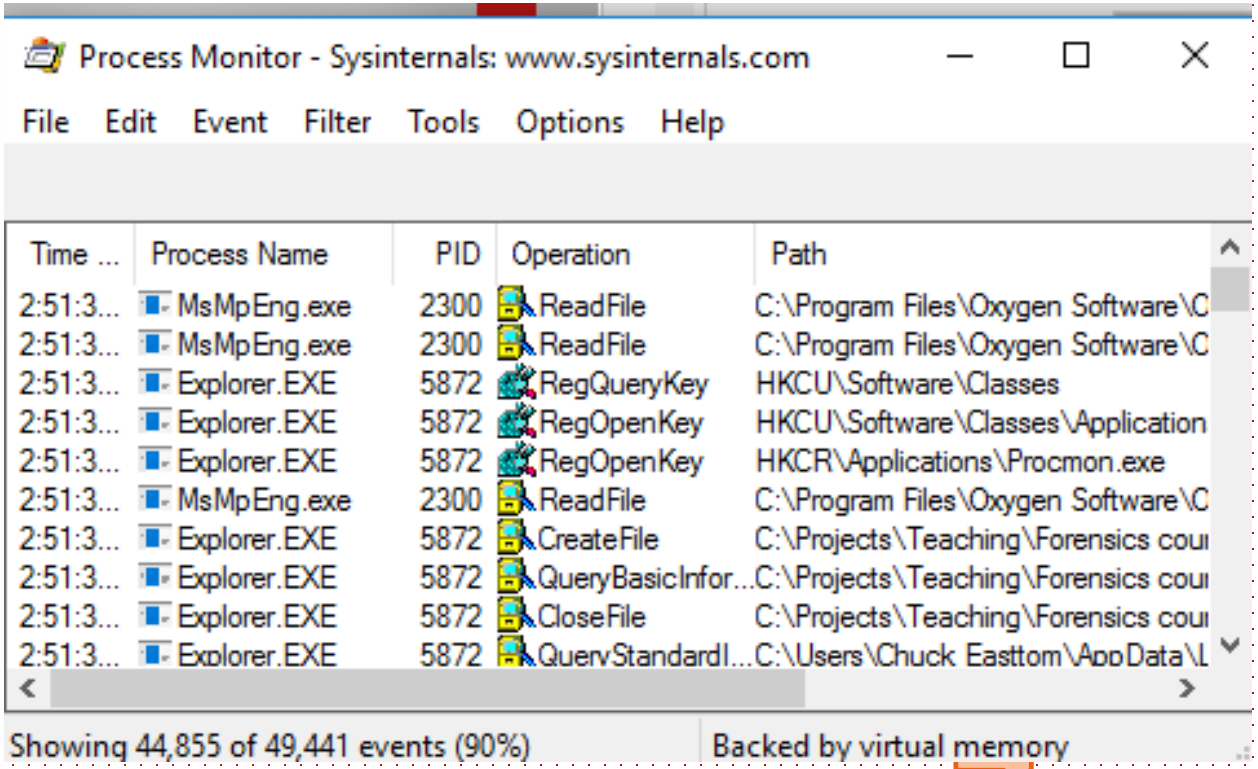
- Rootkitrevealer will not clean the machine, it does, however, scan the hard drive and the registry for possibly problematic files / entries.
- These are then highlighted for the user to take action, if required.

Zero Day

Process Explorer - Sysinternals



Process Monitor - Sysinternals



Zero Day

Questions

www.chuckeasttom.com
chuck@chuckeasttom.com