SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

IR Event Log Analysis

Hal Pomeranz / hal@sans.org / @hal_pomeranz

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Website

digital-forensics.sans.org

SIFT Workstation

dfir.to/SANS-SIFT

Join The SANS DFIR Community

- Blog: dfir.to/DFIRBlog
- Twitter: @sansforensics
- Facebook: sansforensics
- Google+: gplus.to/sansforensics
- Mailing list: dfir.to/MAIL-LIST
- YouTube: dfir.to/DFIRCast

DFIR CURRICULUM

CORE

FOR408
Windows Forensics
GCFE

SEC504
Hacker Techniques, Exploits, and Incident Handling
GCIH

IN-DEPTH INCIDENT RESPONSE

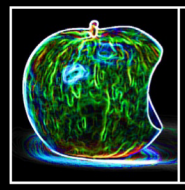
FOR508
Advanced Incident Response
GCFA

FOR572
Advanced Network Forensics and Analysis
GNFA

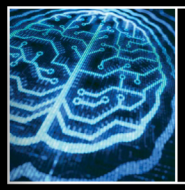
LEARN REM

FOR610
REM: Malware Analysis
GREM

SPECIALIZATION



FOR518
Mac Forensics



FOR526
Memory Forensics In-Depth

MGT535
Incident Response Team Management

FOR585
Advanced Smartphone Forensics

Windows Event Logs

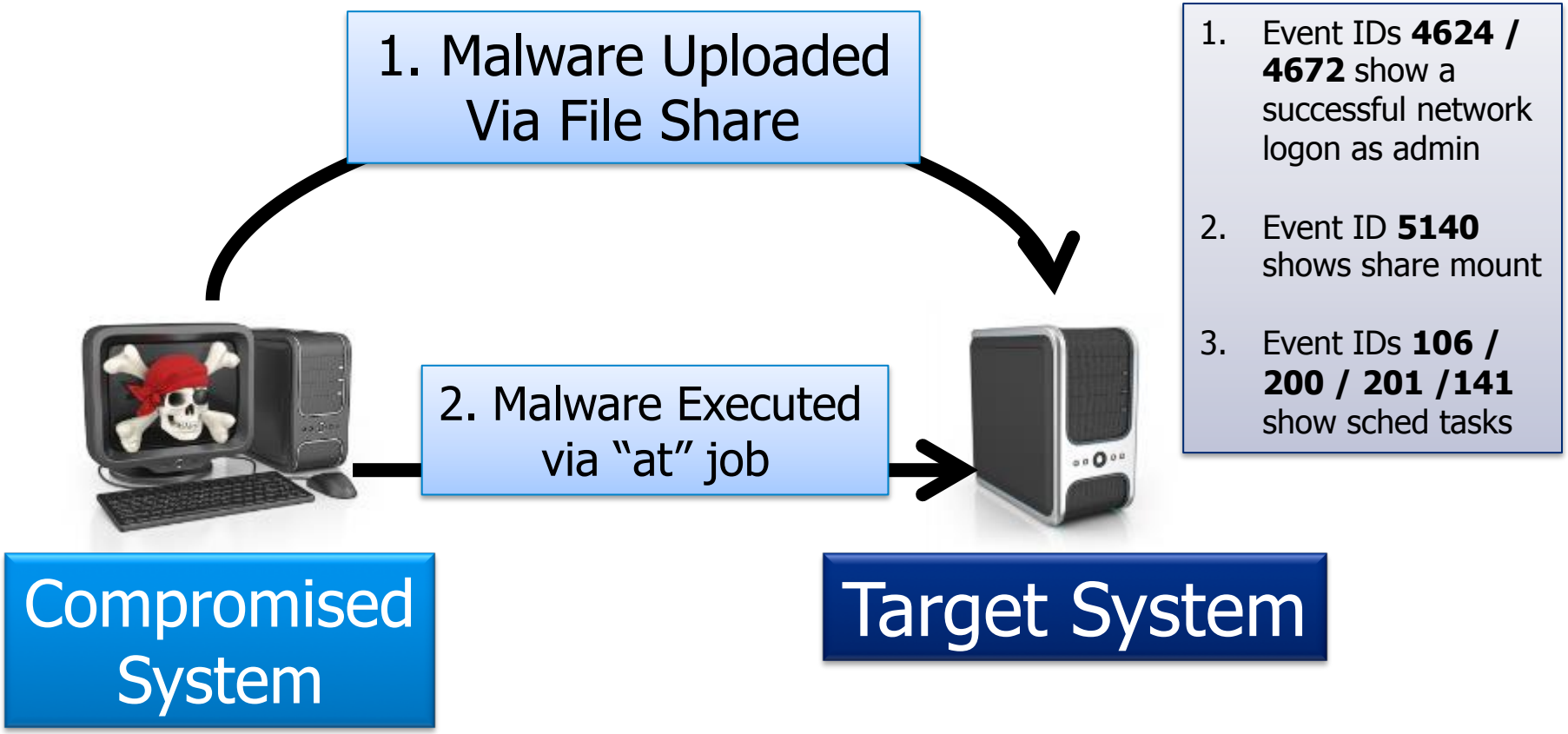
C:\Windows\System32\winevt\Logs.evtx*

Variety of parsers available –

GUI, command-line, and scripty

Analysis is something of a black art?

Example: Lateral Movement



1. Event IDs **4624 / 4672** show a successful network logon as admin
2. Event ID **5140** shows share mount
3. Event IDs **106 / 200 / 201 /141** show sched tasks

Log Timeline

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – Task completed
12:05:41	141 – Task removed
Security.evtx	
12:07:01	4634 – Logoff

Security.evtx	
12:00:00	46
12:00:00	46
12:00:15	51
Microsoft-Win	
12:02:23	10
12:03:00	20
12:03:12	20
12:05:41	14
Security.evtx	
12:07:01	46

Timestamp = 2015-02-14 12:00:00
Event ID = 4624
SubjectUserSid = S-1-0-0
SubjectUserName = -
SubjectDomainName = -
SubjectLogonId = 0x0000000000000000
TargetUserSid = S-1-5-21-2723264887-207281631-482592677-2984
TargetUserName = imowned
TargetDomainName = MYDOM
TargetLogonId = 0x000000021457dbab
LogonType = 3
LogonProcessName = Kerberos
AuthenticationPackageName = Kerberos
WorkstationName =
LogonGuid = {726F6B9E-C1BE-4EC1-BB95-3B0B6238BE56}
TransmittedServices = -
LmPackageName = -
KeyLength = 0
ProcessId = 0x0000000000000000
ProcessName = -
IpAddress = 10.1.1.10
IpPort = 3005

4672 – Admin Rights

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	
Microsoft-	
12:02:23	
12:03:00	
12:03:12	
12:05:41	
Security.e	
12:07:01	4634 – Logoff

Timestamp = 2015-02-14 12:00:00
Event ID = 4672
SubjectUserSid = S-1-5-21-2723264887-207281631-482592677-2984
SubjectUserName = imowned
SubjectDomainName = MYDOM
SubjectLogonId = 0x000000021457dbab
PrivilegeList = SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege
SeTakeOwnershipPrivilege SeDebugPrivilege
SeSystemEnvironmentPrivilege SeLoadDriverPrivilege
SeImpersonatePrivilege SeEnableDelegationPrivilege

5140 – Network Share

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4
12:00:15	5
Microsoft-Wi	
12:02:23	1
12:03:00	2
12:03:12	2
12:05:41	1
Security.evtx	
12:07:01	4

Timestamp = 2015-02-14 12:00:15
Event ID = 5140
SubjectUserSid = S-1-5-21-2723264887-207281631-482592677-2984
SubjectUserName = imowned
SubjectDomainName = MYDOM
SubjectLogonId = 0x000000021457dbab
ObjectType = File
IpAddress = 10.1.1.10
IpPort = 3005
ShareName = //*/C$
ShareLocalPath = /??/C:/
AccessMask = 0x00000001
AccessList: {ReadData (or ListDirectory) }

106 – Task Scheduled

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – Task completed
12:05:41	141 – Task removed
Security.evtx	
12:07:01	4634 – Logoff

Timestamp = 2015-02-14 12:02:23
Event ID = 106
TaskName = /At1
UserContext = MYDOM/imowned

200 – Task Executed

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – T
12:05:41	141 – T
Security.evtx	
12:07:01	4634 – Logon

Timestamp = 2015-02-14 12:03:00
Event ID = 200
TaskName = /At1
ActionName = malicious.bat
TaskInstanceId = {B042B2E4-D186-4970-AE6C-B5DE328BCF3A}

Bonus!

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskSchedul	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – Task completed
12:05:41	141 – Task removed
Security.evtx	
12:07:01	4634 – Logoff

Timestamp = 2015-02-14 12:03:09
Event ID = 4688
SubjectUserSid = S-1-5-18
SubjectUserName = TARGET$
SubjectDomainName = MYDOM
SubjectLogonId = 0x00000000000003e7
NewProcessId = 0x0000000000002318
NewProcessName = C:/Windows/m.exe
TokenElevationType = %%1936
ProcessId = 0x000000000001c04

201 – Task Completed

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – T
12:05:41	141 – T
Security.evtx	
12:07:01	4634 –

Timestamp = 2015-02-14 12:03:12
Event ID = 201
TaskName = /At1
TaskInstanceId = {B042B2E4-D186-4970-AE6C-B5DE328BCF3A}
ActionName = C:/Windows/SYSTEM32/cmd.exe
ResultCode = 0

141 – Task Removed

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106 – Task scheduled
12:03:00	200 – Task executed
12:03:12	201 – Task completed
12:05:41	141 – Task removed
Security.evtx	
12:07:01	4634 – Logoff

Timestamp = 2015-02-14 12:05:41
Event ID = 141
TaskName = /At1
UserName = NT AUTHORITY/System

4634 – Logoff

Security.evtx	
12:00:00	4624 – Network logon
12:00:00	4672 – Admin rights
12:00:15	5140 – Network share
Microsoft-Windows-TaskScheduler%4Operational.evtx	
12:02:23	106
12:03:00	200
12:03:12	201
12:05:41	141
Security.evtx	
12:07:01	4634 – Logoff

Timestamp = 2015-02-14 12:07:01
Event ID = 4634
TargetUserSid = S-1-5-21-2723264887-207281631-482592677-2984
TargetUserName = imowned
TargetDomainName = MYDOM
TargetLogonId = 0x000000021457dbab
LogonType = 3

Review – What Do We Know?

Login events

4624 – Who, where from, time

4672 – They're an admin

5140 – And they mounted a share from …

Scheduled tasks

106 – Job name, who, time

200 – Start time and program name

201 – Finish time

141 – They cleaned up

Example: Domain Controller of Doom!

Malicious RDP activty

Two different RATs

Security.evtx? Not so much…

RDP Event Log Basics

Microsoft-Windows-TerminalServices-RemoteConnectionManager	
13:00:00	1149 – URDOM\owendtu from 192.168.1.10 authenticated
Microsoft-Windows-TerminalServices-LocalSessionManager	
13:00:41	21 – URDOM\owendtu from 192.168.1.10 logon success
14:45:27	23 – URDOM\owendtu logoff
14:45:32	24 – URDOM\owendtu from 192.168.1.10 disconnect

RDP Event Log Permutations

Microsoft-Windows-TerminalServices-RemoteConnectionManager	
15:00:00	1149 – URDOM\owendtu from 192.168.1.10 authenticated
Microsoft-Windows-TerminalServices-LocalSessionManager	
15:00:32	21 – URDOM\owendtu from 192.168.1.10 logon success
Microsoft-Windows-TerminalServices-RemoteConnectionManager	
16:00:00	1149 – URDOM\owendtu from 192.168.100.102 authenticated
Microsoft-Windows-TerminalServices-LocalSessionManager	
16:00:10	25 - URDOM\owendtu from 192.168.100.102 reconnect
16:00:12	24 – URDOM\owendtu from 192.168.1.10 disconnect

Bonus Clue!

Timestamp: 2015-03-17 15:00:12

Event ID: 45 (Symantec Endpoint Protection Client.evtx)

Scan type: Tamper Protection Scan

Event: Tamper Protection Detection

Security risk detected: C:/WINDOWS/SYSWOW64/SVCHOST.EXE

File: C:/Program Files (x86)/Symantec/Symantec Endpoint Protection/12.1.2015.2015.105/Bin64/Smc.exe

Location: C:/Program Files (x86)/Symantec/Symantec Endpoint Protection/12.1.2015.2015.105/Bin64

Computer: OWNDC

User: owendtu

Action taken: Leave Alone

Date found: Tuesday- March 17- 2015 15:00:10

More Malware!

Timestamp = 2015-03-17 16:13:22

Event ID = 7045 (System.evtx)

ServiceName = Nothing to See Here

ImagePath = C:\Windows\Temp\NTSH.exe

ServiceType = user mode service

StartType = auto start

AccountName = LocalSystem

Summary – Other Places to Look

RDP logs last longer than Security.evtx

Application logs can have clues

System.evtx tracks service creation, etc

Wrapping Up

Any final questions?

Can I have that survey link please?

IR Event Log Analysis

Hal Pomeranz / hal@sans.org / @hal_pomeranz