

BSides Zurich 17.09.2016

Advanced Detection using Sysmon

Tom Ueltschi, Swiss Post CERT

C:\> whoami /all

- * Tom Ueltschi
- * Swiss Post CERT / SOC / CSIRT, since 2007
 - Focus: Malware Analysis, Threat Intel, Threat Hunting, Red Teaming
- * Talks about «Ponmocup Hunter» (Botconf, DeepSec, SANS DFIR Summit)
- * Member of many trust groups / infosec communities
- * Twitter: @c_APT_ure

BotConf 2016 Presentation

<https://www.botconf.eu/2016/advanced-incident-detection-and-threat-hunting-using-sysmon-and-splunk/>

[[Download BotConf PDF Slides](#)]

Network- or Host-based Detection?

- * **Network-based Detection (NBD)**

- Intrusion Detection System (IDS) / Network Security Monitoring (NSM)
 - Snort, Surricata , Bro, Security Onion ...

- * **Host-based Detection (HBD)**

- Endpoint Detection and Response (EDR)
 - Carbon Black, FireEye HX, CrowdStrike Falcon, Tanium, RSA ECAT ...
 - **Sysmon (FREE) & Splunk (or any other SIEM)**

- * Discussion

- Is one of {NBD, HBD} enough, better, or are both needed?

Why using Sysmon?

- * **Incredible visibility into system activity** on Windows hosts (it's FREE)
- * Store Sysmon data in Windows event logs (big size)
- * Search or query Sysmon data using Powershell or event viewer
- * **Collect Sysmon logs into SIEM for searching, alerting, hunting** (big plus)
- * Analyst needs to ...
 - know **what to search for**
 - distinguish **normal / abnormal** activity
 - find **suspicious / malicious** behavior

Why Sysmon? RSA Con Talk M.R.

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

HTA-W05

Tracking Hackers on Your Network with Sysinternals Sysmon

Mark Russinovich
CTO, Microsoft Azure
Microsoft Corporation
@markrussinovich

Connect to Protect

#RSAC

The slide features a yellow background with a large, faint outline of a head and a lightbulb. A red vertical bar is on the left, and a purple vertical bar is on the right. A white line connects the top right of the yellow area to the top of the purple area. The purple area contains a globe icon and a crowd of people.

Why Sysmon? RSA Con Talk M.R.

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

Time stomping

DLL / Proc Injection

*Contributed by David Magnotti

7

RSAConference2016

Why Sysmon? RSA Con Talk M.R.

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]
```

Sysmon Event Types: 1 Process create

```
49 TimeCreated : 25.08.2016 11:00:28
50 Id          : 1
51 Message     : Process Create:
52              UtcTime: 2016-08-25 09:00:28.513
53              ProcessGuid: {7622F75A-B3AC-57BE-0000-0010AA46BE02}
54              ProcessId: 9696
55              Image: C:\Windows\System32\cscript.exe
56              CommandLine: "C:\Windows\System32\CScript.exe"
57                  "C:\Users\user\AppData\Local\Temp\Temp1_Rechnung.zip\Rechnung 24.js"
58              CurrentDirectory: C:\Windows\system32\
59              User: DOMAIN\user
60              LogonGuid: {7622F75A-77CB-57BE-0000-0020724B0900}
61              LogonId: 0x94b72
62              TerminalSessionId: 1
63              IntegrityLevel: Medium
64              Hashes: MD5=ECB021CA3370582F0C7244B0CF06732C, IMPHASH=639B19B7E8C7
65                  3FF5646B006D913BA80A
66              ParentProcessGuid: {7622F75A-77DD-57BE-0000-00104DC50A00}
67              ParentProcessId: 4996
68              ParentImage: →:\Windows\Explorer.EXE
69              ParentCommandLine: C:\Windows\explorer.exe
```


Sysmon Event Types: 3 Network connection

```
49 TimeCreated : 25.08.2016 11:00:28
50 Id          : 1
51 Message     : Process Create:
52              UtcTime: 2016-08-25 09:00:28.513
53              ProcessGuid: {7622F75A-B3AC-57BE-0000-0010AA46BE02}
54              ProcessId: 9696
55              Image: C:\Windows\System32\cmd.exe
56              Comm 71 TimeCreated : 25.08.2016 11:00:34
57                  "C 72 Id          : 3
58                  Curr 73 Message     : Network connection detected:
59                  User 74              UtcTime: 2016-08-25 09:00:28.381
60                  Logc 75              ProcessGuid: {7622F75A-B3AC-57BE-0000-0010AA46BE02}
61                  Logc 76              ProcessId: 9696
62                  Tern 77              Image: C:\Windows\System32\cmd.exe
63                  Inte 78              User: DOMAIN\user
64                  Hash 79              Protocol: tcp
65                  3FF5 80              Initiated: true
66                  Pare 81              SourceIsIpv6: false
67                  Pare 82              SourceIp: 10. [REDACTED]
68                  Pare 83              SourceHostname: CLIENT.domain.tld
69                  Pare 84              SourcePort: 63172
69                  Pare 85              SourcePortName:
69                  Pare 86              DestinationIsIpv6: false
69                  Pare 87              DestinationIp: 172. [REDACTED]
69                  Pare 88              DestinationHostname: PROXY.domain.tld
69                  Pare 89              DestinationPort: 3128
69                  Pare 90              DestinationPortName:
```

Why Sysmon? SANS DFIR Poster

SANS DFIR CURRICULUM

CORE

- FOR100 Digital Forensics Fundamentals
- FOR400 Windows Forensics
- FOR500 Advanced Windows Forensics
- SEC204 Incident Response
- GCSE Cyber Security Essentials
- GCSE Cyber Security

IN-DEPTH

- FOR600 Advanced Windows Forensics
- FOR675 Incident Response Forensics
- FOR690 Advanced Windows Forensics
- LEADS REM Memory Forensics
- FOR610 Hacking Windows

SPECIALIZATION

- FOR610 Forensics
- FOR620 Forensics for Cloud
- FOR630 Advanced Windows Forensics

Know Abnormal...Find Evil

Memory Artifacts

Rogue Processes

When searching for anomalies, look for processes that appear abnormal. In an intrusion case, spotting the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

OS Artifacts

Unknown Services

Windows services are designed to run applications in the background without user interaction. These services are managed by the Windows Service Control Manager (SCM) and are listed in the Windows Registry. These services are critical to the system's operation and should be monitored for any changes.

Code Injection and Rootkit Behavior

Code injection and rootkit behavior are techniques used by attackers to gain unauthorized access to a system. These techniques involve injecting malicious code into legitimate processes or installing rootkits that allow the attacker to hide their presence and execute arbitrary code.

Unusual OS Artifacts

Unusual OS artifacts are indicators of abnormal system behavior. These artifacts include suspicious network activity, unusual registry changes, and unusual file system activity. These artifacts can be used to identify potential intrusions and to gather evidence for forensic analysis.

Unusual Windows Behavior:

- Rogue Processes
- Unknown Services
- Code Injection and Rootkit Behavior
- Unusual OS Artifacts
- Suspicious Network Activity
- Evidence of Persistence

Evidence of Persistence

Attackers use various techniques to ensure their access to a system is persistent. These techniques include creating scheduled tasks, registry modifications, and file system changes. These artifacts can be used to identify potential intrusions and to gather evidence for forensic analysis.

Suspicious Network Activity

Suspicious network activity is a key indicator of an intrusion. This activity includes unusual network connections, unusual data transfer volumes, and unusual network protocols. These artifacts can be used to identify potential intrusions and to gather evidence for forensic analysis.

Poster References

- Windows Admin Center, Part 1 & 2
- Windows Admin Center, Part 3
- Windows Admin Center, Part 4
- Windows Admin Center, Part 5
- Windows Admin Center, Part 6
- Windows Admin Center, Part 7
- Windows Admin Center, Part 8
- Windows Admin Center, Part 9
- Windows Admin Center, Part 10
- Windows Admin Center, Part 11
- Windows Admin Center, Part 12
- Windows Admin Center, Part 13
- Windows Admin Center, Part 14
- Windows Admin Center, Part 15
- Windows Admin Center, Part 16
- Windows Admin Center, Part 17
- Windows Admin Center, Part 18
- Windows Admin Center, Part 19
- Windows Admin Center, Part 20
- Windows Admin Center, Part 21
- Windows Admin Center, Part 22
- Windows Admin Center, Part 23
- Windows Admin Center, Part 24
- Windows Admin Center, Part 25
- Windows Admin Center, Part 26
- Windows Admin Center, Part 27
- Windows Admin Center, Part 28
- Windows Admin Center, Part 29
- Windows Admin Center, Part 30
- Windows Admin Center, Part 31
- Windows Admin Center, Part 32
- Windows Admin Center, Part 33
- Windows Admin Center, Part 34
- Windows Admin Center, Part 35
- Windows Admin Center, Part 36
- Windows Admin Center, Part 37
- Windows Admin Center, Part 38
- Windows Admin Center, Part 39
- Windows Admin Center, Part 40
- Windows Admin Center, Part 41
- Windows Admin Center, Part 42
- Windows Admin Center, Part 43
- Windows Admin Center, Part 44
- Windows Admin Center, Part 45
- Windows Admin Center, Part 46
- Windows Admin Center, Part 47
- Windows Admin Center, Part 48
- Windows Admin Center, Part 49
- Windows Admin Center, Part 50
- Windows Admin Center, Part 51
- Windows Admin Center, Part 52
- Windows Admin Center, Part 53
- Windows Admin Center, Part 54
- Windows Admin Center, Part 55
- Windows Admin Center, Part 56
- Windows Admin Center, Part 57
- Windows Admin Center, Part 58
- Windows Admin Center, Part 59
- Windows Admin Center, Part 60
- Windows Admin Center, Part 61
- Windows Admin Center, Part 62
- Windows Admin Center, Part 63
- Windows Admin Center, Part 64
- Windows Admin Center, Part 65
- Windows Admin Center, Part 66
- Windows Admin Center, Part 67
- Windows Admin Center, Part 68
- Windows Admin Center, Part 69
- Windows Admin Center, Part 70
- Windows Admin Center, Part 71
- Windows Admin Center, Part 72
- Windows Admin Center, Part 73
- Windows Admin Center, Part 74
- Windows Admin Center, Part 75
- Windows Admin Center, Part 76
- Windows Admin Center, Part 77
- Windows Admin Center, Part 78
- Windows Admin Center, Part 79
- Windows Admin Center, Part 80
- Windows Admin Center, Part 81
- Windows Admin Center, Part 82
- Windows Admin Center, Part 83
- Windows Admin Center, Part 84
- Windows Admin Center, Part 85
- Windows Admin Center, Part 86
- Windows Admin Center, Part 87
- Windows Admin Center, Part 88
- Windows Admin Center, Part 89
- Windows Admin Center, Part 90
- Windows Admin Center, Part 91
- Windows Admin Center, Part 92
- Windows Admin Center, Part 93
- Windows Admin Center, Part 94
- Windows Admin Center, Part 95
- Windows Admin Center, Part 96
- Windows Admin Center, Part 97
- Windows Admin Center, Part 98
- Windows Admin Center, Part 99
- Windows Admin Center, Part 100

Know Normal...Find Evil

Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware. Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

System

Image Path: %SystemRoot%\System32\cmd.exe
Parent Process: System
Member of Instance: One
Process: System Idle Process
Start Time: When loaded into memory

csrss.exe

Image Path: %SystemRoot%\System32\csrss.exe
Parent Process: System
Member of Instance: One
Process: csrss.exe
Start Time: When loaded into memory

smss.exe

Image Path: %SystemRoot%\System32\smss.exe
Parent Process: System
Member of Instance: One
Process: smss.exe
Start Time: When loaded into memory

wininit.exe

Image Path: %SystemRoot%\System32\wininit.exe
Parent Process: System
Member of Instance: One
Process: wininit.exe
Start Time: When loaded into memory

taskhost.exe

Image Path: %SystemRoot%\System32\taskhost.exe
Parent Process: System
Member of Instance: One
Process: taskhost.exe
Start Time: When loaded into memory

lsass.exe

Image Path: %SystemRoot%\System32\lsass.exe
Parent Process: System
Member of Instance: One
Process: lsass.exe
Start Time: When loaded into memory

winlogon.exe

Image Path: %SystemRoot%\System32\winlogon.exe
Parent Process: System
Member of Instance: One
Process: winlogon.exe
Start Time: When loaded into memory

explorer.exe

Image Path: %SystemRoot%\System32\explorer.exe
Parent Process: System
Member of Instance: One
Process: explorer.exe
Start Time: When loaded into memory

services.exe

Image Path: %SystemRoot%\System32\services.exe
Parent Process: System
Member of Instance: One
Process: services.exe
Start Time: When loaded into memory

svchost.exe

Image Path: %SystemRoot%\System32\svchost.exe
Parent Process: System
Member of Instance: One
Process: svchost.exe
Start Time: When loaded into memory

lsism.exe

Image Path: %SystemRoot%\System32\lsism.exe
Parent Process: System
Member of Instance: One
Process: lsism.exe
Start Time: When loaded into memory

winlogon.exe

Image Path: %SystemRoot%\System32\winlogon.exe
Parent Process: System
Member of Instance: One
Process: winlogon.exe
Start Time: When loaded into memory

explorer.exe

Image Path: %SystemRoot%\System32\explorer.exe
Parent Process: System
Member of Instance: One
Process: explorer.exe
Start Time: When loaded into memory

explorer.exe

Image Path: %SystemRoot%\System32\explorer.exe
Parent Process: System
Member of Instance: One
Process: explorer.exe
Start Time: When loaded into memory

Why Sysmon? SANS DFIR Poster

SANS DFIR CURRICULUM

DIGITAL FORENSICS & INCIDENT RESPONSE

POSTER

SPRING 2014 - 20TH EDITION

digital-forensics.sans.org

Know Abnormal...Find Evil

Know Normal...Find Evil

Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware. Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

System

Image Path: ** - Not generated from a trustworthy image

Parent Process: Not

Number of Instances: One

User Account: Local System

Start Time: At boot time

Description: The csrss.exe process is designed to use hardware acceleration, but only processes that support Direct3D can do so. This process is used to launch Direct3D applications.

csrss.exe

Image Path: %systemroot%\system32\csrss.exe

Parent Process: csrss.exe

Number of Instances: Two or more

User Account: Local System

Start Time: Within seconds of boot time for the parent process

Description: The csrss.exe process is designed to use hardware acceleration, but only processes that support Direct3D can do so. This process is used to launch Direct3D applications.

services.exe

Image Path: %systemroot%\system32\services.exe

Parent Process: smss.exe

Number of Instances: One

User Account: Local System

Start Time: Within seconds of boot time for the parent process

Description: The services.exe process is responsible for starting and stopping Windows services.

Process Hacker

Hacker View Tools Users Help

Refresh Options Search Processes (Ctrl+F)

Processes Services Network Disk

Name

- System Idle Process
- System
- Interrupts

When searching for malicious processes, look for any of these anomalous characteristics:

- Started with the wrong parent process
- Image executable is located in the wrong path
- Misspelled processes
- Processes that are running under the wrong account (incorrect SID)
- Processes with unusual start times (i.e., starts minutes or hours after boot when it should be within seconds of boot)
- Unusual command-line arguments
- Packed executables

Why Sysmon? SANS DFIR Poster

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
POSTER
SPRING 2014 - 20TH EDITION
digital-forensics.sans.org

Know Abnormal

Memory Artifacts

In an intrusion case, the difference between abnormal and normal is often the difference between success and failure. Your mission is to quickly identify suspicious artifacts in order to verify potential intrusions. Use the information below as a reference for locating anomalies that could reveal the actions of an attacker.

When searching for anomalous artifacts, look for any of these:

- Started with unusual parent process
- Image executed under the wrong account (incorrect SID)
- Used start times (i.e., starts minutes or hours ahead of boot)
- Used arguments

Rogue Processes

Malware authors frequently seek out system processes to hijack and use as a means of evasion. When searching for rogue processes, look for any of the following:

- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager

Code Injection and Shellcode

Code injection and shellcode are techniques used by attackers to execute arbitrary code on a target system. When searching for code injection and shellcode, look for any of the following:

- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager

Suspicious Network

Malware authors frequently seek out system processes to hijack and use as a means of evasion. When searching for suspicious network activity, look for any of the following:

- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager
- Processes that are not listed in the Windows Task Manager

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
Know Normal...Find Evil
Knowing what's normal on a Windows host helps cut through the noise to quickly locate potential malware. Use the information below as a reference to know what's normal in Windows and to focus your attention on the outliers.

csrss.exe

Image Path: %systemroot%\system32\csrss.exe
Parent Process: Created by an instance of smss.exe that exits its subject task immediately after the parent process exits.
Number of Instances: Two or more
User Account: Local System
Start Time: Make record of how long for the first instance to start. If you see additional instances occur, you may notice an offset, although also only a few seconds. If you are correct, the description of the process is the same as the first instance. In Windows Task Manager, the description of the process is the same as the first instance. In Windows Task Manager, the description of the process is the same as the first instance. In Windows Task Manager, the description of the process is the same as the first instance.

services.exe

Image Path: %systemroot%\system32\services.exe
Parent Process: smssinit.exe
Number of Instances: One
User Account: Local System

any of these

Processes that are not listed in the Windows Task Manager

Processes that are not listed in the Windows Task Manager

Processes that are not listed in the Windows Task Manager

Why Sysmon? SANS DFIR Poster

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
POSTER
SPRING 2014 - 20TH EDITION
digital-forensics.sans.org

Know About

Memory Artifacts

Rogue Processes

Code Injection and Rootkit Behavior

Suspicious Network Activity

svchost.exe

Image Path: %SystemRoot%\System32\svchost.exe

Parent Process: services.exe

Number of Instances: Five or more

User Account: Varies depending on svchost instance, though it typically will be Local System, Network Service, or Local Service accounts. Instances running under any other account should be investigated.

Start Time: Typically within seconds of boot time. However, services can be started after boot, which might result in new instances of svchost.exe well after boot time.

Description: The generic host process for Windows Services. It is used for running service DLLs. Windows will run multiple instances of svchost.exe, each using a unique "-k" parameter for grouping similar services. Typical "-k" parameters include BTsvcs, DcomLaunch, RPCSS, LocalServiceNetworkRestricted, netsvcs, LocalService, NetworkService, LocalServiceNoNetwork, secsvcs, and LocalServiceAndNoImpersonation. Malware authors often take advantage of the ubiquitous nature of svchost.exe and use it either directly or indirectly to hide their malware. They use it directly by installing the malware as a service in a legitimate instance of svchost.exe. Alternatively, they use it indirectly by trying to blend in with legitimate instances of svchost.exe, either by slightly misspelling the name (e.g., scvhost.exe) or spelling it correctly but placing it in a directory other than System32. Keep in mind that a legitimate svchost.exe should always run from %SystemRoot%\System32, should have services.exe as its parent, and should host at least one service. Also, on default installations of Windows 7, all service executables and all service DLLs are signed by Microsoft.

Find Evil

normal in Windows and to focus your attention on the outliers.

Look for any of these

csrss.exe

services.exe

svchost.exe

lsism.exe

explorer.exe

Why Sysmon? SANS DFIR Poster

alert_sysmon_suspicious_svchost

```
index=it_bapo SourceName="Microsoft-Windows-Sysmon" EventCode=1
  svchost.exe
| search Image="*\svchost.exe*"
  CommandLine!="* -k *" OR
  (Image!="C:\\Windows\\System32\\svchost.exe"
    Image!="C:\\Windows\\SysWOW64\\svchost.exe") OR
  ParentImage!="*:\\Windows\\system32\\services.exe"
```

- * Search for «svchost.exe» process created
 - Without «-k» parameter
 - Parent process is not «services.exe»
 - Running under wrong path

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection

G+ 1

f Like 9

🐦 Tweet

in Share 16



ANDRA
ZAHARIA
MARCOM MANAGER



JULY 4TH, 2016 • 17:15

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection

 1

 Like 9

 Tweet

 Share 16



ANDRA
ZAHARIA
MARCUM MANAGER




SHA256: 7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0

File name: Doc-172394856.jar

Detection ratio: 0 / 52

Analysis date: 2016-07-04 07:45:42 UTC (1 day, 2 hours ago) [View latest](#)

JULY 4T

 Analysis

 File detail

 Additional information

 Comments 2

 Votes

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection



ANDRA
ZAHARIA
MARCUM MANAGER



JULY 4T



SHA256: 7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0

File name: 7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0.bin

Detection ratio: 8 / 55

Analysis date: 2016-07-05 10:18:08 UTC (10 minutes ago)



SHA256

Analysis

File detail

Additional information

Comments 2

Votes

File name

Antivirus

Result

Update

AegisLab

Backdoor.Java.Agent!c

20160705

Detection

ESET-NOD32

Java/Adwind.VX

20160705

Analysis

Ikarus

Trojan.Java.Adwind

20160705

Kaspersky

Backdoor.Java.Agent.aw

20160705

McAfee-GW-Edition

Artemis

20160705

Microsoft

Backdoor.Java/Adwind.R

20160705

TrendMicro

JAVA_ADWIND.DUC

20160705

TrendMicro-HouseCall

JAVA_ADWIND.DUC

20160705

Analys

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection



ANDRA
ZAHARIA
MARCOM MANAGER



JULY 4T



SHA256: 7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0
File name: 7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0.bin
Detection ratio: 8 / 55
Analysis date: 2016-07-05 10:18:08 UTC (10 minutes ago)



SH [Analysis](#) [File detail](#) [Additional information](#) [Comments](#) 2 [Votes](#)

File #Adwind
De

Posted 1 day, 1 hour ago by CSISkruse

An



submitname:"7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0"
vxstream-threatscore:79/100
domains:"jmcoru.alcatelupd.xyz"
hosts:"77.81.104.169:6050"
source:<https://www.hybrid-analysis.com/sample/7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0?environmentId=100>

Posted 1 day, 2 hours ago by PayloadSecurity

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection

The image shows a social media post on the left and a web browser window on the right. The social media post features a profile picture of Andra Zaharia, MarcCom Manager, and a 'Like' button. The browser window displays the Payload Security website, showing a security alert for a file named 'Doc-172394856.jar'. The alert details include the analysis date (July 4th 2016), the system used (Windows 7), and the report generated by VxStream Sandbox. Below the alert, there are buttons for 'Login to Download Sample (255KiB)', 'Downloads', 'VirusTotal Report', and 'Re-analyze'. The 'Incident Response' section is expanded to show a 'Risk Assessment' table.

Incident Response	
Risk Assessment	
Remote Access	Uses network protocols on unusual ports
Persistence	Spawns a lot of processes
Network Behavior	Contacts 1 domain and 1 host. View the network section for more details.

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection

PAYLOAD SECURITY Home Submissions Resources Contact

Hybrid Analysis

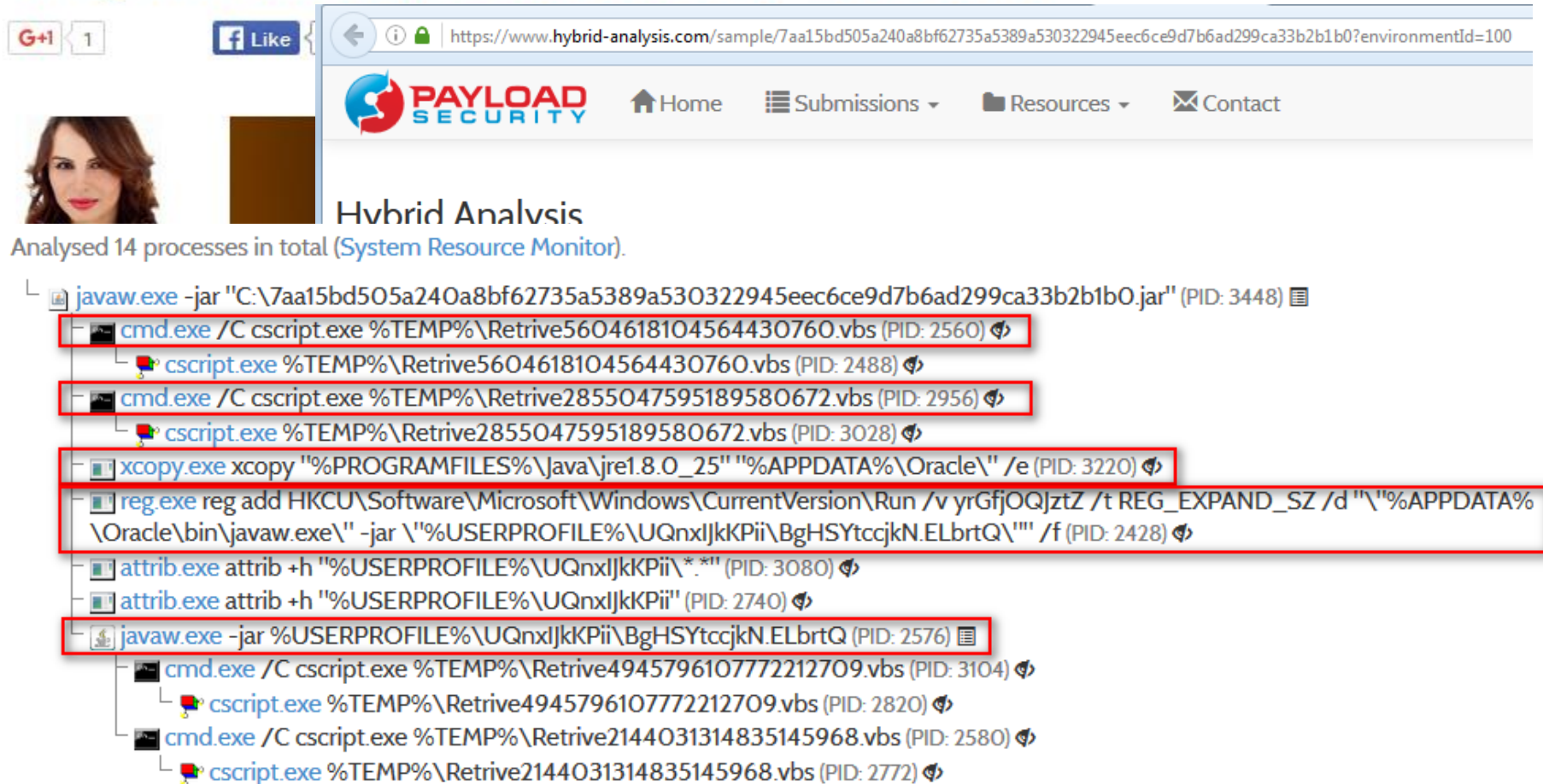
Tip: Click an analysed process below to view more details.

Analysed 14 processes in total (System Resource Monitor).

- javaw.exe -jar "C:\7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0.jar" (PID: 3448)
 - cmd.exe /C csript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2560)
 - csript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2488)
 - cmd.exe /C csript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 2956)
 - csript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 3028)
 - xcopy.exe xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e (PID: 3220)
 - reg.exe reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v yrGfjOQJztZ /t REG_EXPAND_SZ /d "\"%APPDATA%\Oracle\bin\javaw.exe\" -jar \"%USERPROFILE%\UQnxlJkKpii\BgHSYtccjkN.ELbrtQ\" /f (PID: 2428)
 - attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKpii*.*)" (PID: 3080)
 - attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKpii" (PID: 2740)
 - javaw.exe -jar %USERPROFILE%\UQnxlJkKpii\BgHSYtccjkN.ELbrtQ (PID: 2576)
 - cmd.exe /C csript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 3104)
 - csript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 2820)
 - cmd.exe /C csript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2580)
 - csript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2772)

Why Sysmon? Advanced Detection

Security Alert: Adwind RAT Spotted in Targeted Attacks with Zero AV Detection



Analysed 14 processes in total (System Resource Monitor).

- javaw.exe -jar "C:\7aa15bd505a240a8bf62735a5389a530322945eec6ce9d7b6ad299ca33b2b1b0.jar" (PID: 3448)
 - cmd.exe /C cscript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2560)
 - cscript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2488)
 - cmd.exe /C cscript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 2956)
 - cscript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 3028)
 - xcopy.exe xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e (PID: 3220)
 - reg.exe reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v yrGfjOQJztZ /t REG_EXPAND_SZ /d "\"%APPDATA%\Oracle\bin\javaw.exe\" -jar \"%USERPROFILE%\UQnxlJkKPi\BgHSYtccjK.N.ELbrtQ\" /f (PID: 2428)
 - attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPi*" (PID: 3080)
 - attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPi" (PID: 2740)
 - javaw.exe -jar %USERPROFILE%\UQnxlJkKPi\BgHSYtccjK.N.ELbrtQ (PID: 2576)
 - cmd.exe /C cscript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 3104)
 - cscript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 2820)
 - cmd.exe /C cscript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2580)
 - cscript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2772)

Why Sysmon? Advanced Detection

alert_sysmon_java-malware-infection

```
index=sysmon SourceName="Microsoft-Windows-Sysmon" EventCode="1"  
(Users AppData Roaming (javaw.exe OR xcopy.exe)) OR (cmd cscript vbs) |  
search Image="*\\AppData\\Roaming\\Oracle\\bin\\java*.exe*"  
OR (Image="*\\xcopy.exe*" CommandLine="*\\AppData\\Roaming\\Oracle\\*")  
OR CommandLine="*cscript*Retrieve*.vbs*"
```

Analysed 14 processes in total (System Resource Monitor).

The screenshot shows a process tree for `javaw.exe` (PID: 3448). The following processes are highlighted with red boxes:

- `cmd.exe /C cscript.exe %TEMP%\Retrieve5604618104564430760.vbs (PID: 2560)`
- `cscript.exe %TEMP%\Retrieve5604618104564430760.vbs (PID: 2488)`
- `cmd.exe /C cscript.exe %TEMP%\Retrieve2855047595189580672.vbs (PID: 2956)`
- `cscript.exe %TEMP%\Retrieve2855047595189580672.vbs (PID: 3028)`
- `xcopy.exe xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e (PID: 3220)`
- `reg.exe reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v yrGfjOQJztZ /t REG_EXPAND_SZ /d "%APPDATA%\Oracle\bin\javaw.exe" -jar "%USERPROFILE%\UQnxlJkKPii\BgHSYtccjK.N.ELbrtQ\" /f (PID: 2428)`
- `attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPii*" (PID: 3080)`
- `attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPii" (PID: 2740)`
- `javaw.exe -jar %USERPROFILE%\UQnxlJkKPii\BgHSYtccjK.N.ELbrtQ (PID: 2576)`
- `cmd.exe /C cscript.exe %TEMP%\Retrieve4945796107772212709.vbs (PID: 3104)`
- `cscript.exe %TEMP%\Retrieve4945796107772212709.vbs (PID: 2820)`
- `cmd.exe /C cscript.exe %TEMP%\Retrieve2144031314835145968.vbs (PID: 2580)`
- `cscript.exe %TEMP%\Retrieve2144031314835145968.vbs (PID: 2772)`

Why Sysmon? Advanced Detection

alert_sysmon_persistence_reg_add

```
index=it_bapo SourceName="Microsoft-Windows-Sysmon" EventCode=1
  reg.exe add CurrentVersion |
search
  Image="*\reg.exe"
  CommandLine="* add *" CommandLine="*CurrentVersion\Run*"
```

Analysed 14 processes in total (System Resource Monitor).

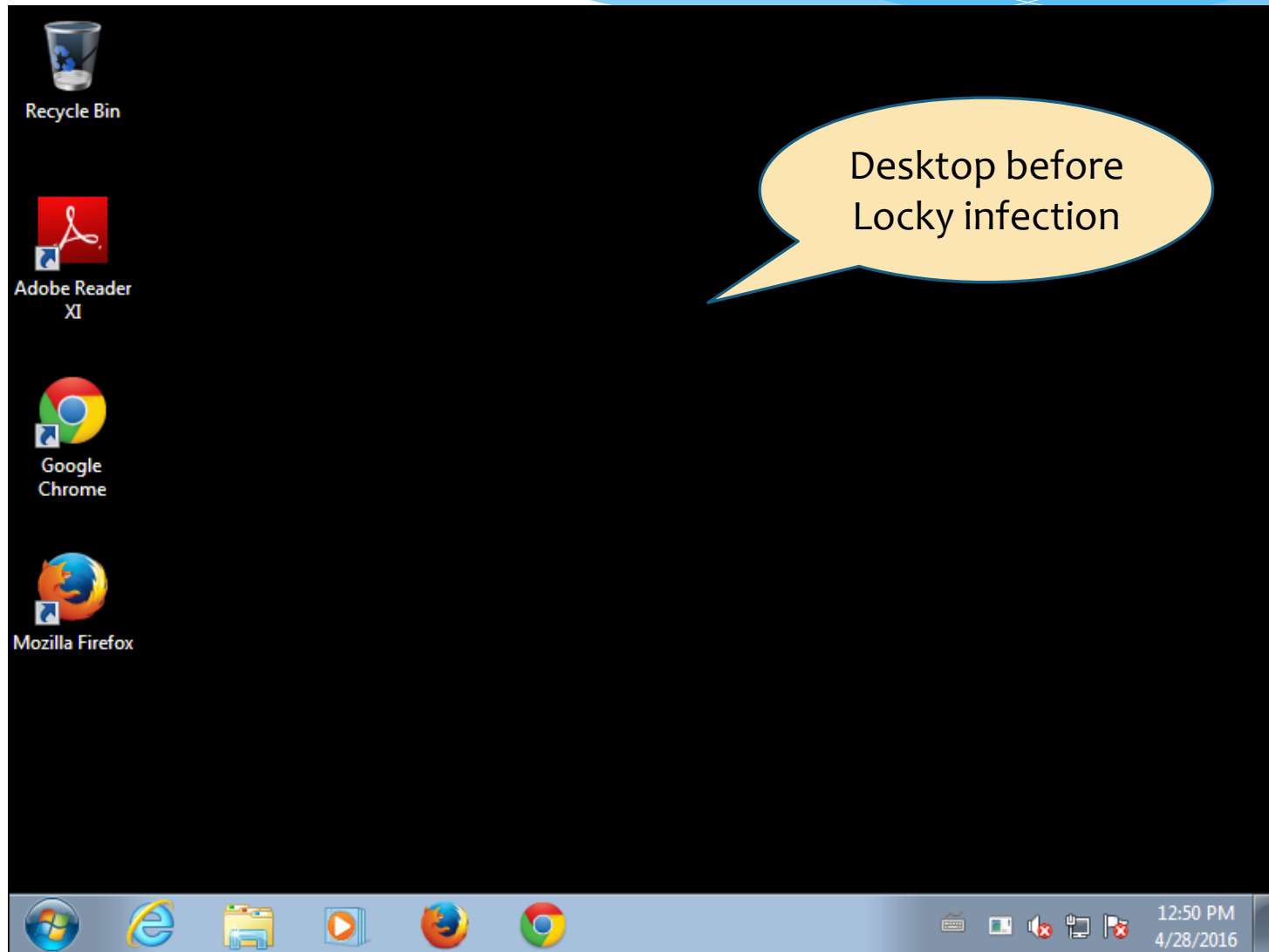
The screenshot displays a process tree for `javaw.exe` (PID: 3448). The following processes are highlighted with red boxes:

- `cmd.exe /C cscript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2560)`
- `cscript.exe %TEMP%\Retrive5604618104564430760.vbs (PID: 2488)`
- `cmd.exe /C cscript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 2956)`
- `cscript.exe %TEMP%\Retrive2855047595189580672.vbs (PID: 3028)`
- `xcopy.exe xcopy "%PROGRAMFILES%\Java\jre1.8.0_25" "%APPDATA%\Oracle\" /e (PID: 3220)`
- `reg.exe reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v yrGfjOQJztZ /t REG_EXPAND_SZ /d "%APPDATA%\Oracle\bin\javaw.exe" -jar "%USERPROFILE%\UQnxlJkKPi\BgHSYtccjK.N.ELbrtQ\" /f (PID: 2428)`
- `attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPi*" (PID: 3080)`
- `attrib.exe attrib +h "%USERPROFILE%\UQnxlJkKPi" (PID: 2740)`
- `javaw.exe -jar %USERPROFILE%\UQnxlJkKPi\BgHSYtccjK.N.ELbrtQ (PID: 2576)`
- `cmd.exe /C cscript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 3104)`
- `cscript.exe %TEMP%\Retrive4945796107772212709.vbs (PID: 2820)`
- `cmd.exe /C cscript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2580)`
- `cscript.exe %TEMP%\Retrive2144031314835145968.vbs (PID: 2772)`

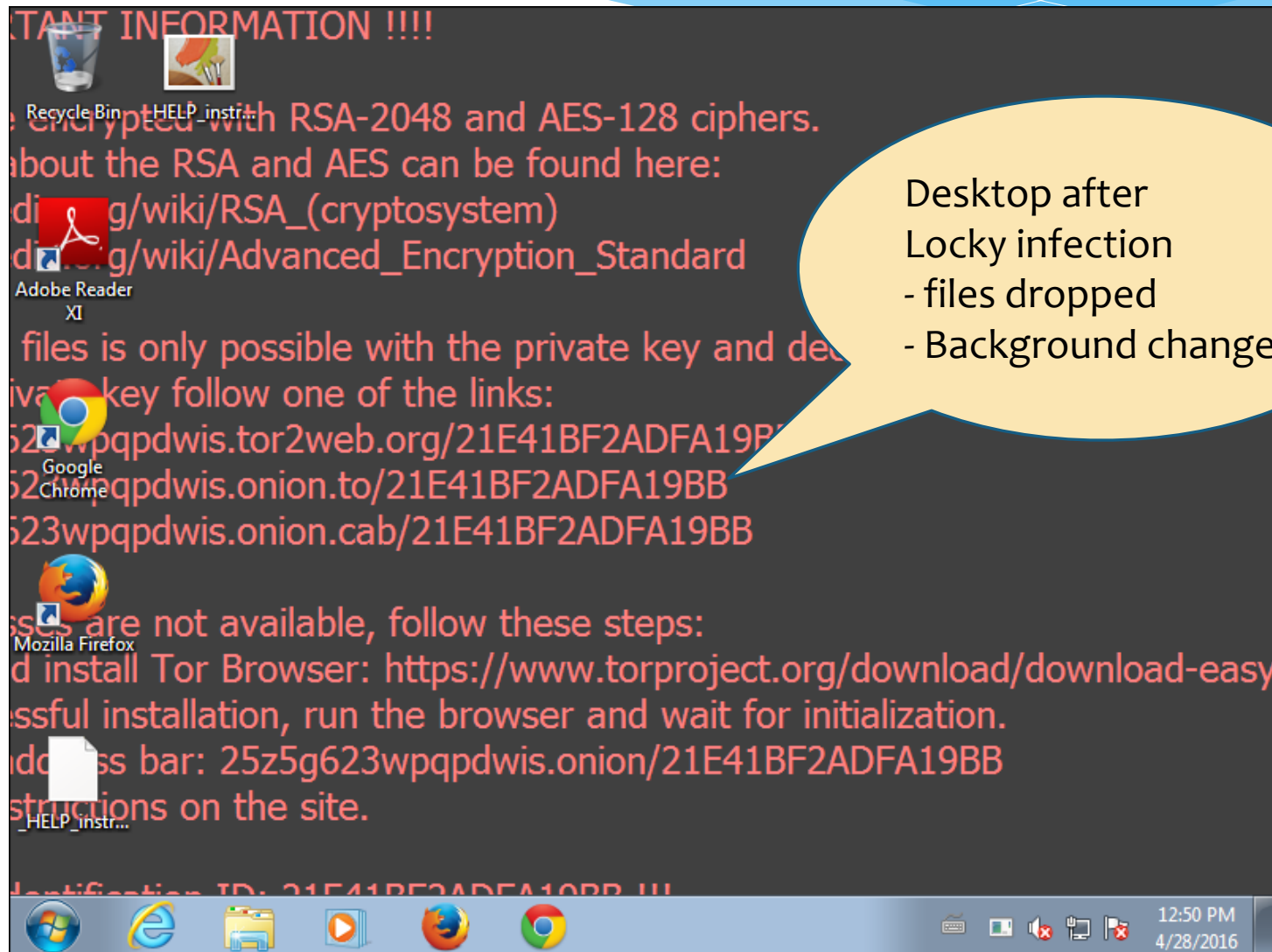
Detecting Locky Ransomware

- * Continuously analysing malspam samples (semi-autom. malware analysis)
 - Ransomware (Locky, Cerber, Tesla et.al.)
 - Dridex, info- / password-stealers, RATs
- * Know malicious behavior (e.g. process tree, command lines)
- * **Detect changes in behavior, adjust searches & alerts accordingly**
- * Comparing two Locky samples from April and August 2016
 - Behavior changed (Vssadmin vs. Rundll32)

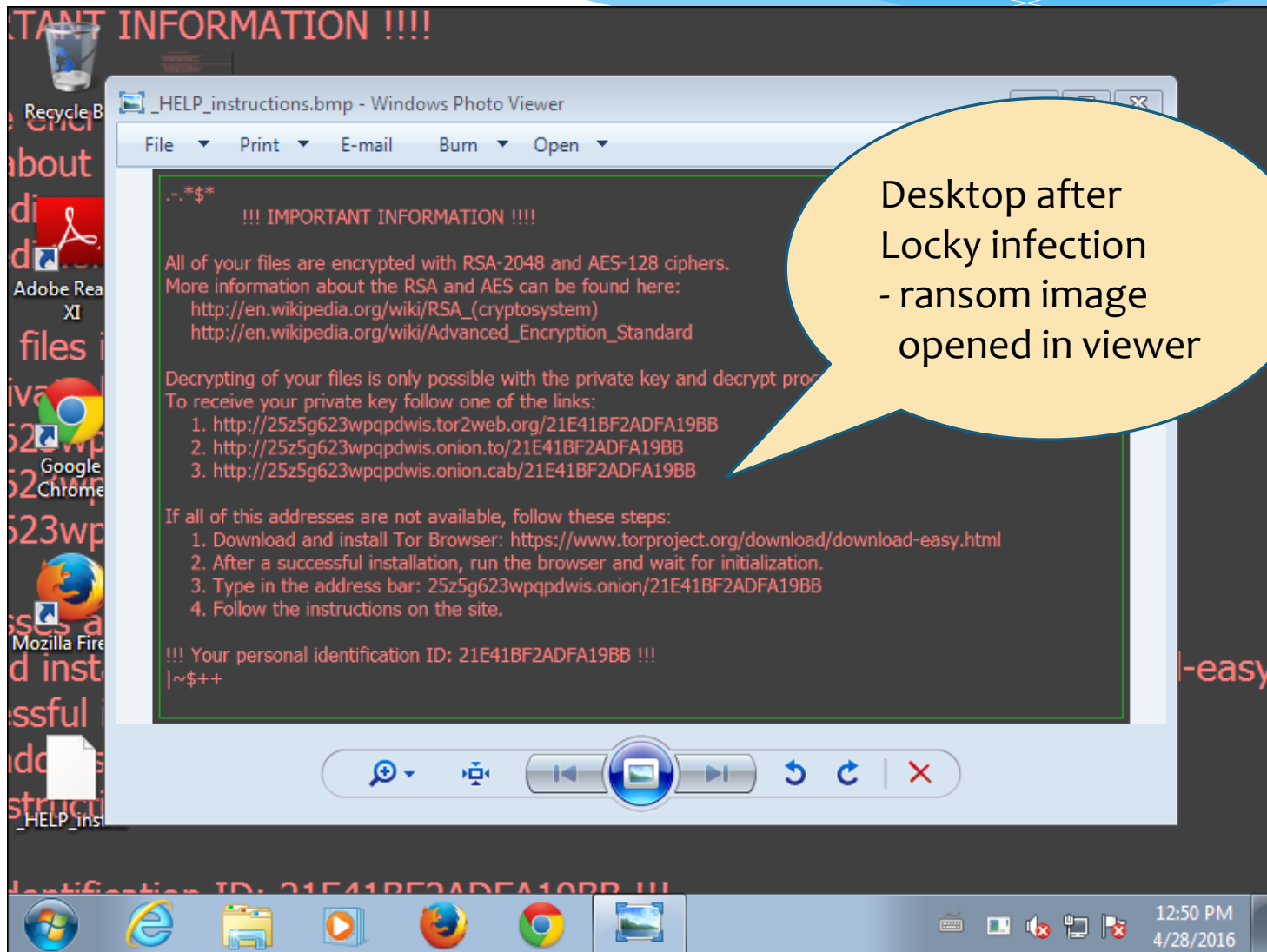
Locky analysis 2016-04-28



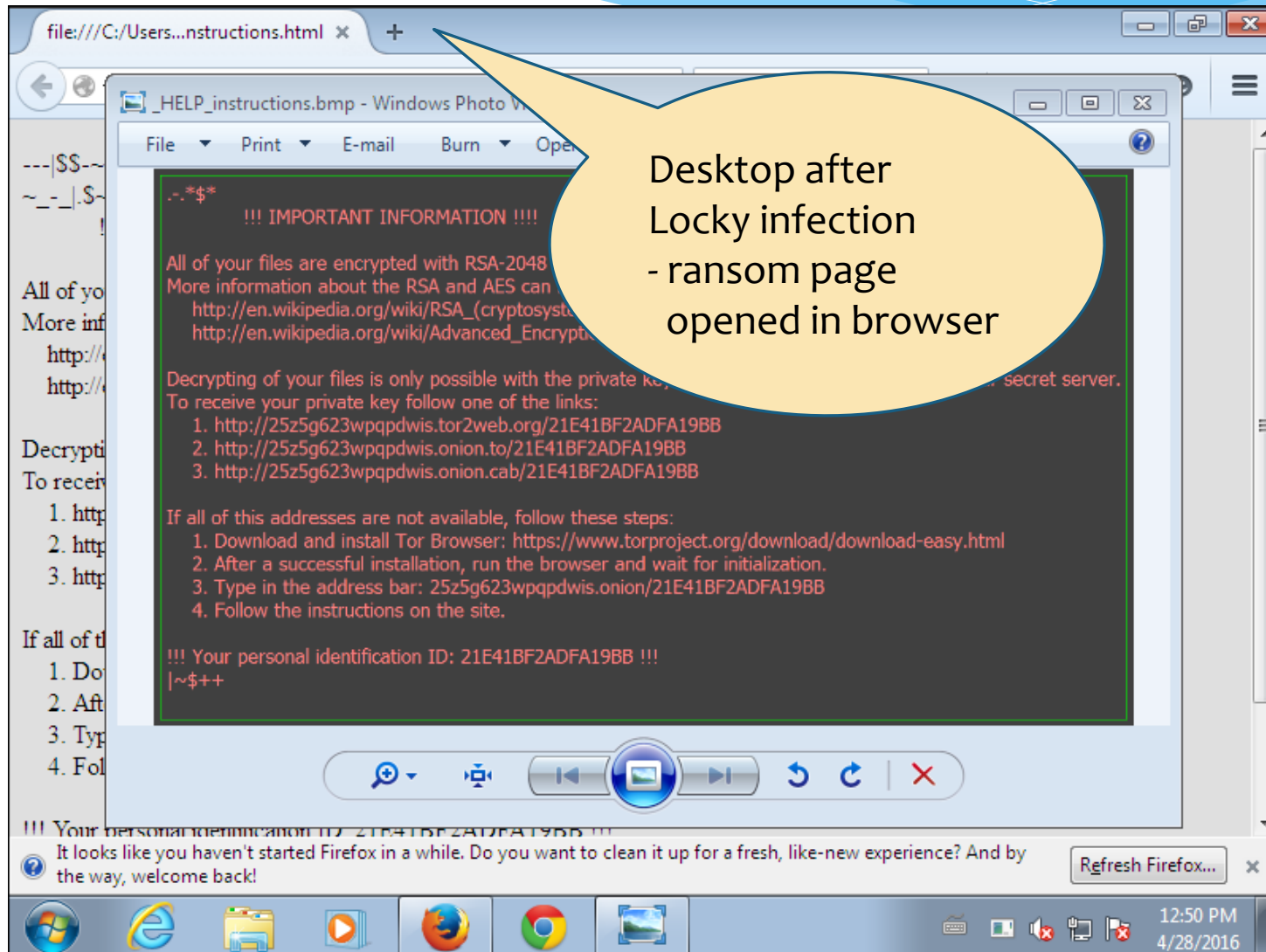
Locky analysis 2016-04-28



Locky analysis 2016-04-28



Locky analysis 2016-04-28



Locky analysis 2016-04-28

Startup

- **system is w7_2**
- **wscript.exe** (PID: 2600 MD5: 979D74799EA6C8B8167869A68DF5204A)
 - **nuNvDiKt.exe** (PID: 808 MD5: 628D9F2BA204F99E638A91494BE3648E)
 - **nuNvDiKt.exe** (PID: 3572 MD5: 628D9F2BA204F99E638A91494BE3648E)
 - **vssadmin.exe** (PID: 3932 MD5: 6E248A3D528EDE43994457CF417BD665)
 - **firefox.exe** (PID: 2480 MD5: F51D682701B303ED6CC5474CE5FA5AAA)
 - **cmd.exe** (PID: 180 cmdline: `cmd.exe /C del /Q /F C:\Users\admin\AppData\Local\Temp\nuNvDiKt.exe`)
- **svchost.exe** (PID: 3892 MD5: 54A47F6B5E09A77E61649109C6A08866)
- **cleanup**

- * `pid="808" / md5="628D9F2BA204F99E638A91494BE3648E" / parentpid="2600" cmdline="C:\Users\admin\AppData\Local\Temp\nuNvDiKt.exe"`
- * `pid="3572" / md5="628D9F2BA204F99E638A91494BE3648E" / parentpid="808" cmdline="C:\Users\admin\AppData\Local\Temp\nuNvDiKt.exe"`
- * `pid="3932" / md5="6E248A3D528EDE43994457CF417BD665" / parentpid="3572" cmdline="vssadmin.exe Delete Shadows /All /Quiet"`
- * `pid="2480" / md5="F51D682701B303ED6CC5474CE5FA5AAA" / parentpid="3572" cmdline="C:\Program Files\Mozilla Firefox\firefox.exe -osint -url C:\Users\admin\Desktop_HELP_instructions.html"`

Locky anal

JOE Sandbox Cloud PRO

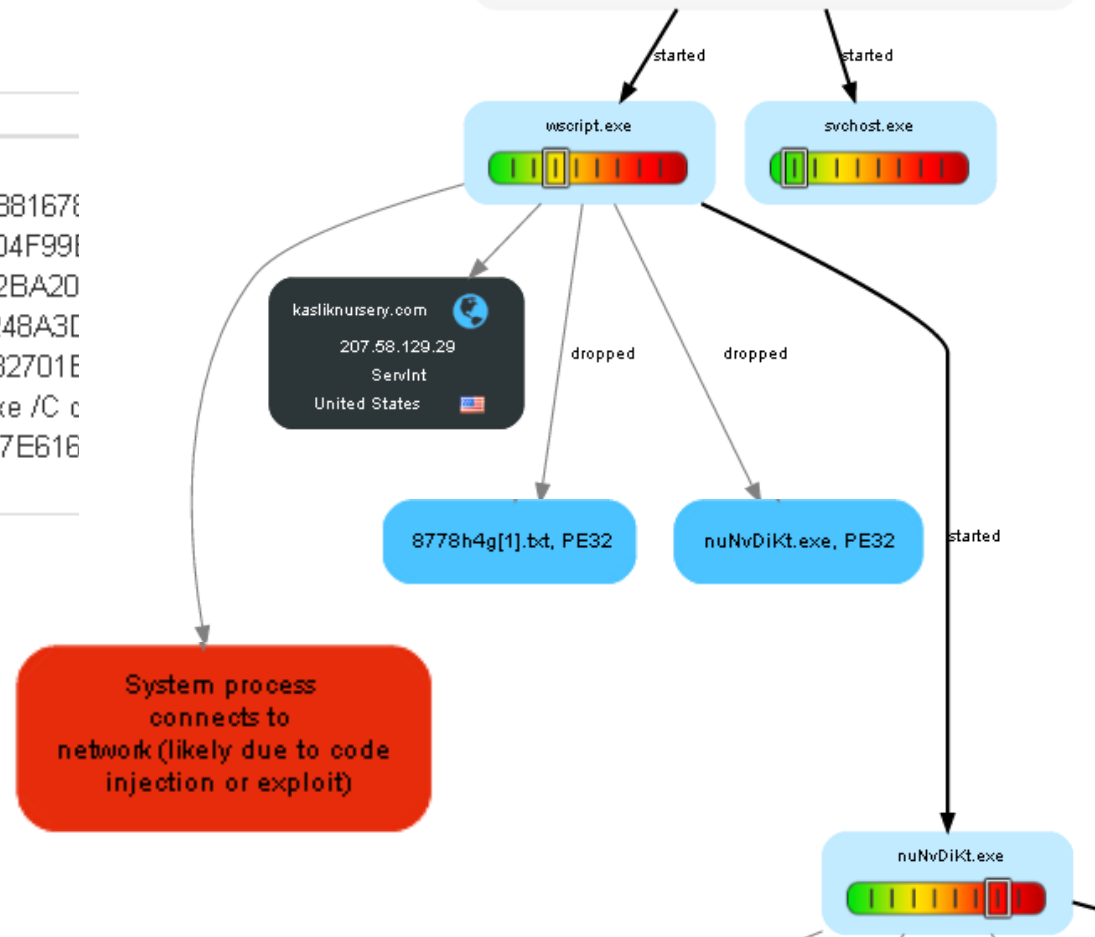
Startup

- **system is w7_2**
- **wscript.exe** (PID: 2600 MD5: 979D74799EA6C8B8167E)
 - **nuNvDiKt.exe** (PID: 808 MD5: 628D9F2BA204F99E)
 - **nuNvDiKt.exe** (PID: 3572 MD5: 628D9F2BA20)
 - **vssadmin.exe** (PID: 3932 MD5: 6E248A3C)
 - **firefox.exe** (PID: 2480 MD5: F51D682701E)
 - **cmd.exe** (PID: 180 cmdline: cmd.exe /C c
- **svchost.exe** (PID: 3892 MD5: 54A47F6B5E09A77E616)
- **cleanup**

Behavior Graph

ID:	120746
Sample:	001834107.js
Startdate:	28/04/2016
Architecture:	WINDOWS
Score:	100

The score indicator shows three stacked boxes: a red box labeled 'MALICIOUS', a yellow box labeled 'SUSPICIOUS', and a green box labeled 'CLEAN'. The 'MALICIOUS' box is the top-most and is highlighted.



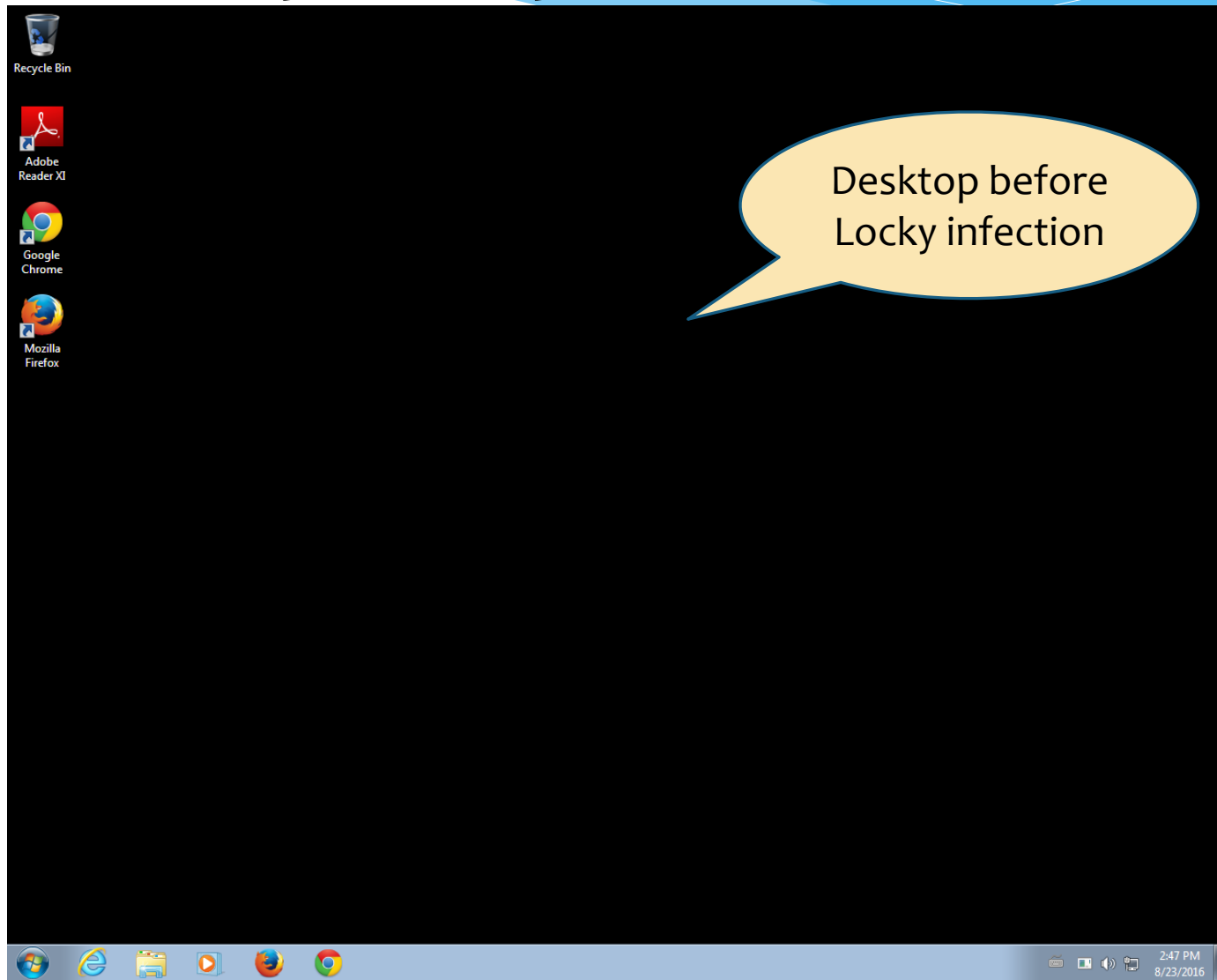
Locky using Vssadmin

- * Locky calling vssadmin to delete shadow copies

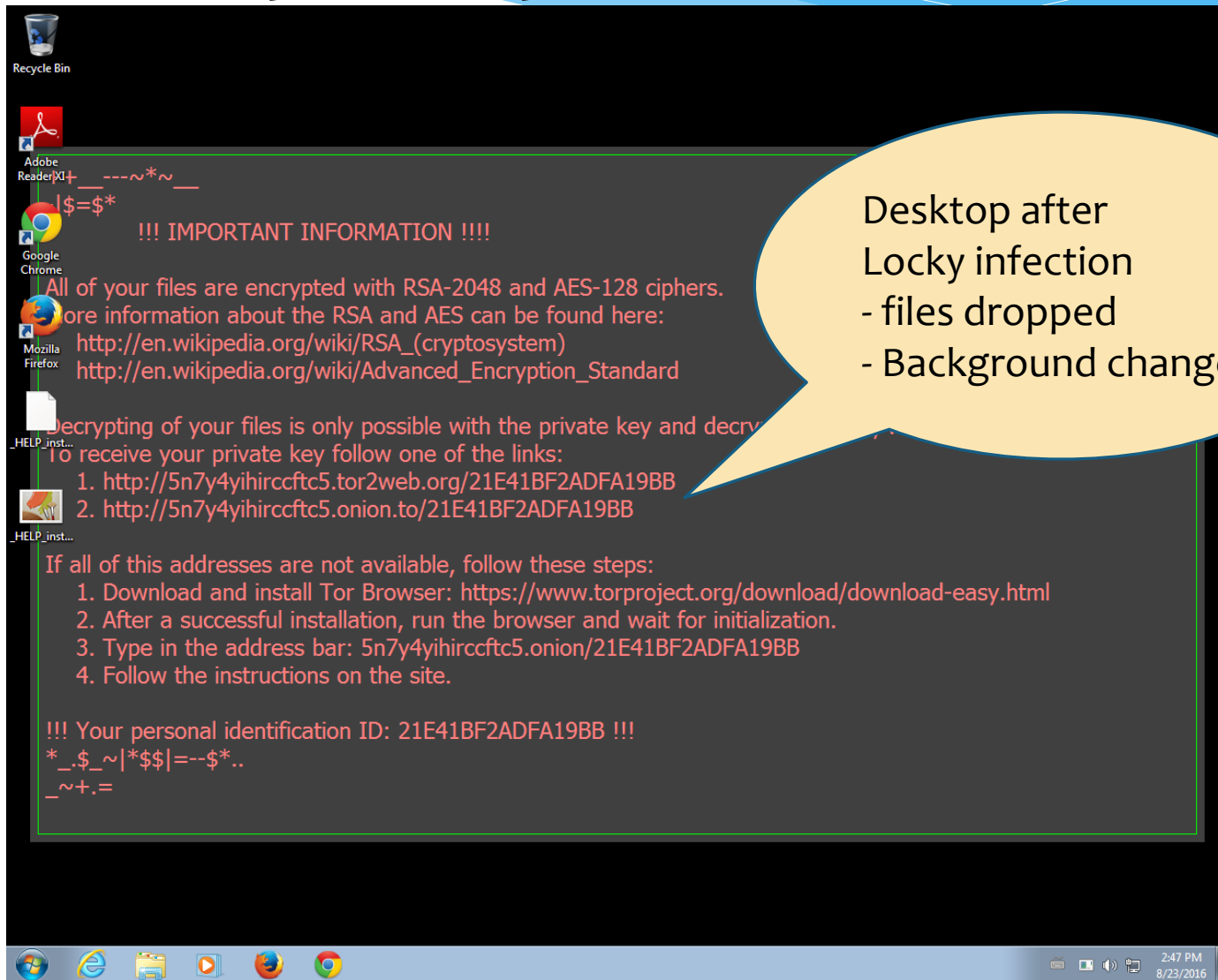
alert_sysmon_vssadmin_ransomware

```
index=sysmon SourceName="Microsoft-Windows-Sysmon" EventCode=1  
  vssadmin.exe  
| search CommandLine="*vssadmin*" EventCode=1  
  CommandLine="*Delete *" CommandLine="*Shadows*" EventCode=1
```

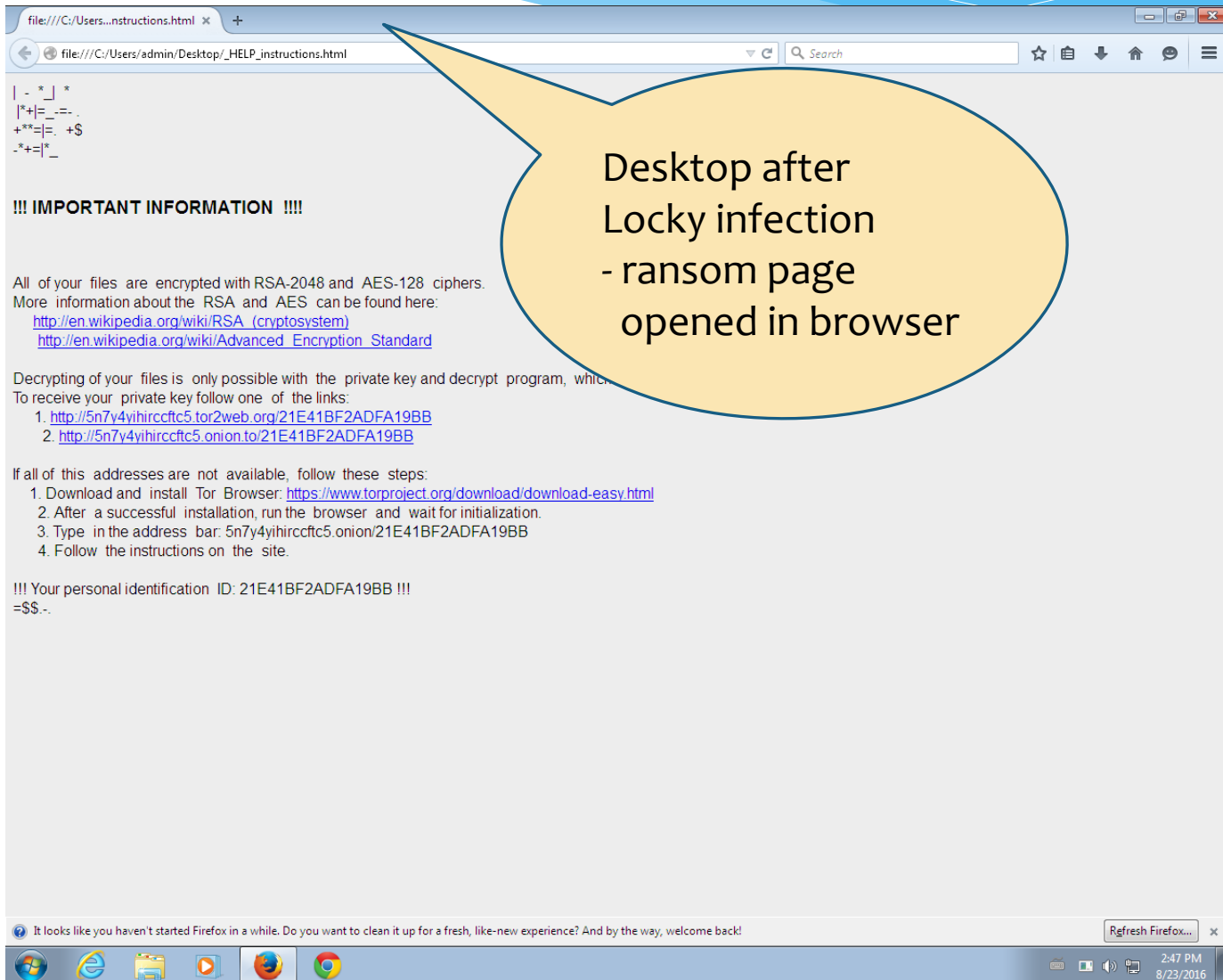
Locky analysis 2016-08-23



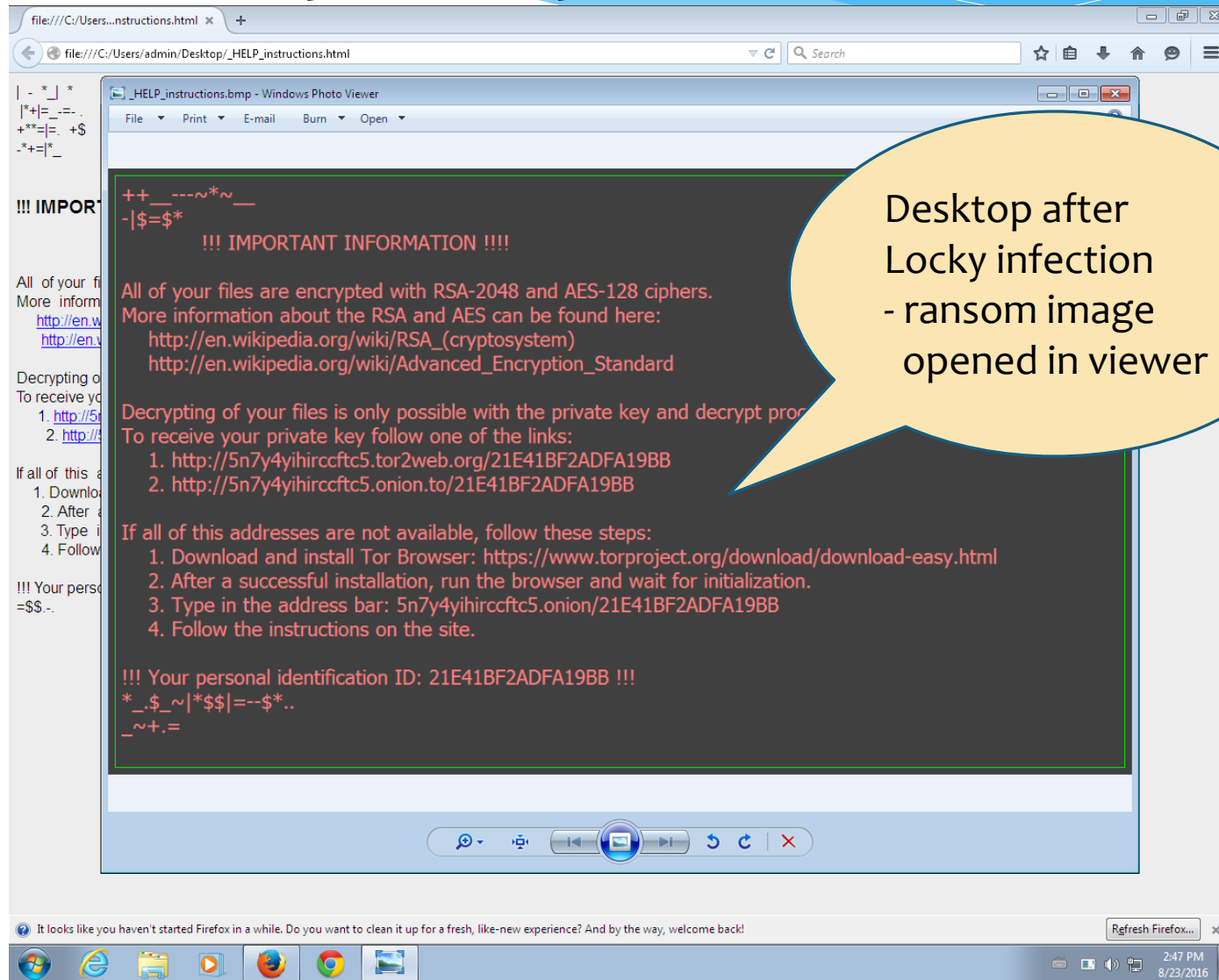
Locky analysis 2016-08-23



Locky analysis 2016-08-23



Locky analysis 2016-08-23



Locky analysis 2016-08-23

- **system is w7_2**
- **wscript.exe** (PID: 4028 MD5: 979D74799EA6C8B8167869A68DF5204A)
 - **rundll32.exe** (PID: 2240 cmdline: C:\Windows\System32\rundll32.exe C:\Users\admin\AppData\Local\Temp\CHJGDH~1.DLL qwerty 323 MD5: 51138BEEA3E2C21EC44D0932C71762A8)
 - **firefox.exe** (PID: 2504 MD5: F51D682701B303ED6CC5474CE5FA5AAA)
- **cleanup**

- system is
- wscript.exe
 - rundll
 - C:\Ue
 - 5113E
 - fi
- cleanup

Behavior Graph

ID: 158275

Sample: audit_report_c456d23b.js

Startdate: 23/08/2016

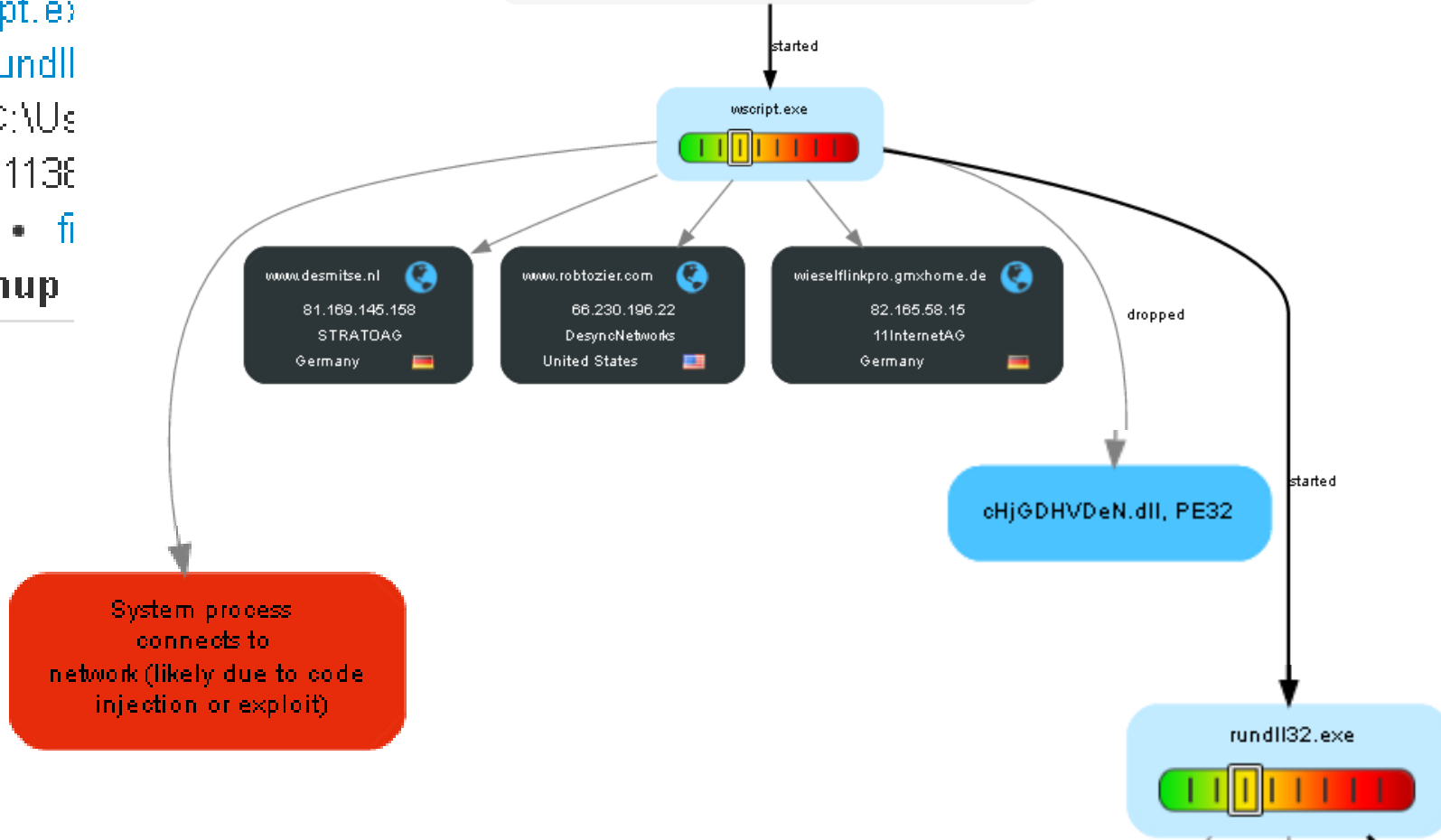
Architecture: WINDOWS

Score: 88

MALICIOUS

SUSPICIOUS

CLEAN



Locky using Rundll32

- * Rundll32 process with
 - DLL in «%TEMP%» folder and «qwerty» parameter
 - Office (macros) or scripting parent process (JS, VBS, WSF, HTA)

alert_sysmon_suspicious_locky_rundll32

```
index=sysmon SourceName="Microsoft-Windows-Sysmon" EventCode=1  
rundll32.exe  
| search Image="*\\rundll32.exe"  
  (CommandLine="*\\AppData\\Local\\Temp" CommandLine="* qwerty") OR  
  (ParentImage="*\\winword.exe" OR ParentImage="*\\excel.exe" OR  
  ParentImage="*\\cscript.exe" OR ParentImage="*\\wscript.exe" OR  
  ParentImage="*\\mshta.exe")
```

Locky Blog 6 days later



TrendLabs  SECURITY
INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

[Home](#)

[Categories](#)

[Home](#) » [Malware](#) » [Locky Ransomware Now Downloaded as Encrypted DLLs](#)

Locky Ransomware Now Downloaded as Encrypted DLLs

Posted on: [August 29, 2016](#) at 4:56 am **Posted in:** [Malware](#), [Ransomware](#)

Author: [Brooks Li \(Threats Analyst\)](#)

Locky Blog 6 days later

After de-obfuscation, we can see that the code does several things:

1. There is a hardcoded list of malicious URLs which all host the encrypted Locky ransomware. The JavaScript will randomly select one URL to download from, if this fails it will try another one.
2. Save the downloaded file content to %temp%
3. Using XOR with a pseudo-random number generator (PRNG) to decrypt the downloaded file and save the decrypted results as xxx.dll
4. Using *rundll32.exe* to run the malicious DLL, which will result in the ransom note being displayed and the user's files being encrypted.

In effect, the attacker created his own stream cipher as his source of a pseudorandom key stream. All PRNGs rely on an initial value (known as the seed) to set the generator's initial state. In a normal cryptographic implementation, so long as this value is non-constant and the PRNG is well designed, the stream cipher will be sufficiently "random".

Posted on: August 29, 2016 at 4:56 am **Posted in:** Malware, Ransomware

Author: Brooks Li (Threats Analyst)

Locky Blog 6 days later

«... attempt to try to evade behavior monitoring features [...] of modern endpoint security products.»

we can see that the code does several things:

which all host the encrypted Locky ransomware. to download from, if this fails it will try another

2. Save the decrypted file content to %temp%

3. Using XorShift pseudo-random number generator (PRNG) to decrypt the downloaded file and save the results as xxx.dll

4. Using rundll32.exe to run the malicious DLL, which will result in the ransom note being displayed and the user's files being encrypted.

In effect, the attacker created his own stream cipher as his source of a pseudorandom key stream. All PRNGs rely on an initial value (known as the seed) to set the generator's initial state. In a normal cryptographic implementation, so long as this value is non-constant and the PRNG is well

Using a DLL file in this way represents an attempt to try and evade behavior monitoring features that are now part of modern endpoint security products. Running as a DLL prevents a new process from being started, making it harder to detect. Other ransomware families (like CryptMIC/CryptXXX) have used this tactic as well, although for Locky this is new.

The use of encryption is also meant to strengthen this malware's ability to hide itself. Without receiving the right parameters from the downloader, no actual malicious file is actually decrypted (and theoretically, detected).

Threat Hunting using Sysmon

blog.sqrrl.com/threat-hunter-profile-bianco

Aug 1, 2016 5:45:22 PM

Threat Hunter Profile - David Bianco

Editor's Note: This is the first in a series of posts that will profile various threat hunters, highlighting their experiences, as well as hunting techniques and lessons from the field.



Name: David J. Bianco

Organization: Sqrrl

Years hunting: 8

Favorite datasets: HTTP proxy logs, authentication logs, process data

Favorite hunting techniques: Outlier detection, visualization

Favorite tools: Sqrrl, Unix command line, Python, Apache Spark, scikit-learn

Threat Hunting using Sysmon

blog.sqrri.com/threat-hunter-profile-bianco

Aug 1, 2016 5:45:22 PM

Threat Hunter Profile - David Bianco

Who are you?

My name is David J. Bianco, and I'm the Lead Security Technologist at Sqrri.

How would you define Threat Hunting?

I define it as the collective name for various techniques used to discover malicious activity in an IT environment that the automated detection systems missed. The key to this definition is that hunting always involves a human. If it's fully automated, it's not hunting!

However, I also think that the purpose of hunting ideally is to improve your automated detection. If your hunting techniques work, automate them so you don't have to keep doing the same hunts over and over again. You'll find things more quickly that way, and you'll be able to spend your time improving your hunting!

Organization: Sqrri

Years hunting: 8

Favorite datasets: HTTP proxy logs, authentication logs, process data

Favorite hunting techniques: Outlier detection, visualization

Favorite tools: Sqrri, Unix command line, Python, Apache Spark, scikit-learn

Threat Hunting using Sysmon

www.threathunting.net

The ThreatHunting Project

Hunting for adversaries in your IT
environment

Threat Hunting using Sysmon

www.threathunting.net

T
T
P

/ Procedures Indexed by Goal

// 0-day Exploits

EMET Log Mining

// **Attacker tools in use**

Suspicious Process Creation via Windows Event Logs

Windows Service Analysis

Psexec Windows Events

Hunting for adversaries in your IT environment

Threat Hunting using Sysmon

www.threathunting.net

T
T
P

/ Procedures Indexed by Goal

- // O-day
 - Psexec Windows Events
 - EMET L
 - Detecting Lateral Movement in Windows Event Logs
- // Attac
 - RDP External Access
 - Suspici
 - Windows Lateral Movement via Explicit Credentials
 - Window
 - Lateral Movement Detection via Process Monitoring
 - Psexec
- // Malicious Listening Services
 - Search for Rogue Listeners

Hunting for
environment

Threat Hunting using Sysmon

www.threathunting.net

T

// Procedures Indexed by Goal

// O-day

EMET L

// Attac

Suspici

Windov

Psexec

// Lateral movement / Compromised Credentials

Psexec Windows Events

Detecting Lateral Movement in

RDP External Access

Windows Lateral Movement via Explicit Credentials

Lateral Movement Detection via Process Monitoring

// Privilege Escalation

Privileged Group Tracking

// Malicious Listening Services

Search for Rogue Listeners

Hunting for
environment

Threat Hunting using Sysmon

www.threathunting.net

Lateral Movement Detection via Process Monitoring

Purpose

Find threat actors moving laterally in the network by looking for examples of common techniques they use to orient themselves on new systems.

Data Required

Windows process creation logs (security event 4688) or other similar information (e.g., EDR logs)

Collection Considerations

The more endpoints and servers from which you collect process information, the more likely you are to be able to find threat actor activity.

Analysis Techniques

- Counting occurrences within a time window

Description

Several legitimate windows binaries executing within a specified time frame may indicate lateral movement.

Threat Hunting using Sysmon

www.threathunting.net

Lateral Movement Detection via Process Monitoring

Description

Several legitimate windows binaries executing within a specified time frame may indicate lateral movement.

As an adversary moves from machine to machine they will often want to know things like: who they are, what level of access do they have, what services are running on the machine, what other machines are around them... They will often determine this by using legitimate windows binaries. When determining this information they will typically do this in minutes vs hours regardless if they are using a script or typing the commands on a command line. Knowing this, we can use it to our advantage. Again focusing on windows event logs and focusing on event codes 4688/592 try to identify the following:

- net.exe, ipconfig.exe, whoami.exe, nbtstat.exe...
- Cluster x number of processes executing within a 10 minute time frame.

For the data that is returned:

- identify the parent process and if it's legitimate?
- What additional processes have executed on the machine within a 1 hour period and do any of those look suspicious? If there are, are they owned by the same user?
- Are these spawned by the same process or process name?
- Are these processes all owned by the same user?
- Is there previous history of this activity?"

Threat Hunting using Sysmon

www.threathunting.net

Suspicious Process Creation via Windows Event Logs

Purpose

Find attacker tools in use

Data Required

Windows process creation logs (Event 4688 & 592)

Collection Considerations

Collect these from every host in the domain. If you have additional endpoint data collection tools that can log data about process execution (e.g. Microsoft Sysmon, Carbon Black, etc) you may be able to similar analyses with equivalent data.

Analysis Techniques

stack counting

Description

Search all process creation log entries and look for:

- `svchost.exe` processes that are not children of `services.exe`

Threat Hunting using Sysmon

www.threathunting.net

Suspicious Process Creation via Windows Event Logs

Purpose

Find attacker tools in use

Data Required

Windows process creation logs (Event 4688 & 592)

Collection Considerations

Collect these from every host in the domain. If you execute Sysmon (e.g. Microsoft Sysmon, Carbon Black, etc)

Analysis Techniques

stack counting

Description

Search all process creation log entries and look for:

- `svchost.exe` processes that are not children of `services.exe`

Description

Search all process creation log entries and look for:

- `svchost.exe` processes that are not children of `services.exe`
- Processes created by binaries in unusual locations, such as
 - `%windows%\fonts`
 - `%windows%\help`
 - `%windows%\wbem`
 - `%windows%\addins`
 - `%windows%\debut`
 - `%windows%\system32\tasks`
- Known attacker tool names, such as
 - `rar.exe`
 - `psexec.exe`
 - `whoami.exe`

- Processes that launched very few times during a 24 hour period

Threat Hunting using Sysmon

www.threathunting.net

T

Suspicious Process Creation via Windows Event Logs

Description

Purpose

Find attacker tools in use

Search all process creation log entries and look for:

- `svchost.exe` processes that are not children of `services.exe`
- Processes created by binaries in unusual locations, such as
 - `%windows%\fonts`

Data Required

Windows process creation logs (Event 4688 & 592)

Other Notes

Event 4688 is even more valuable if logging policy is set to record the entire command line (some of these suggestions require that info). Review your domain audit policies and/or supplement with additional process logging as necessary. Sysmon is a very good free tool that can do nearly anything you'd need.

«Sysmon is a very good free tool that can do nearly anything you'd need»

Thank you for your attention!
Questions during discussion

Tom Ueltschi, Swiss Post CERT