WildFire Analysis Report

1 File Information

File Type	PE
File Signer	Patch My PC 3rd Party Application Component
SHA-256	71fd58f193e40c448c8c8eeeb735d2130df8ca1826b8df8cadc131ec84b68bf2
SHA-1	8209edb8ccaf488be2efc9a90c646b615adb5779
MD5	d7ae64fea3a36683ea1cd789e90473b0
File Size	43344848bytes
First Seen Timestamp	2020-03-27 13:21:15 UTC
Verdict	**Malware**
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Contains a TLS section

Thread-local storage (TLS) is normally used to manage data in multithreaded applications. However, it can also allow execution of code outside of the expected entry point of a PE file.

Contains overlay data

Overlay data is extra data appended to the end of a PE image. Many legitimate files, including all files that are digitally signed, contain overlay data. However, malware often uses overlays to embed encoded or encrypted data as well.

Contains non-standard section names

Standard section names are defined by the compiler. Non-standard section names may indicate a packed or obfuscated PE file.

Contains an unusual entry point

The entry point of a PE file is the starting address for execution. An unusually located entry point may indicate a packed or obfuscated file.

Contains sections with zero size

Sections with zero size indicate a packed or obfuscated PE file.

3 Dynamic Analysis

3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Modified Portable Executable image sections at runtime Portable Executable images contain sections with different access and execution permissions. These sections are built statically during compilation, and runtime modifications indicate binary obfuscation techniques.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	

3.1.2. Network Activity

No network data available.

3.1.3. Host Activity

Process Activity

Process Name - sample.exe

(command: c:\documents and settings\administrator\sample.exe)

Process Activity

Child Process	Action
"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-OHI79.tmp\yrmsacifh.tmp" /SL5="$700DA,42518203,401920,c:\documents and settings\administrator\sample.exe"	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-OHI79.tmp\yrmsacifh.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

Created Mutexes

Mutex Name
oleacc-msaa-loaded
CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500

CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

Process Name - yrmsacifh.tmp

(command: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-OHI79.tmp\yrmsacifh.tmp" /SL5="$700DA,42518203,401920,c:\documents and settings\administrator\sample.exe")

Created Mutexes

Mutex Name
oleacc-msaa-loaded
CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

Event Timeline

1	Created Process c:\documents and settings\administrator\sample.exe
2	Created mutex oleacc-msaa-loaded
3	Created file C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-OHI79.tmp\yrmsacifh.tmp
4	Created mutex CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
5	Created mutex CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
6	Created mutex CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
7	Created mutex CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
8	Created mutex CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
9	Created mutex CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500
10	Created Process "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\is-OHI79.tmp\yrmsacifh.tmp" /SL5="$700DA,42518203,401920,c:\documents and settings\administrator\sample.exe"
11	Created mutex oleacc-msaa-loaded
12	Created mutex CTF.LBES.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
13	Created mutex CTF.Compart.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
14	Created mutex CTF.Asm.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
15	Created mutex CTF.Layouts.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
16	Created mutex CTF.TMD.MutexDefaultS-1-5-21-515967899-776561741-1417001333-500
17	Created mutex CTF.TimListCache.FMPDefaultS-1-5-21-515967899-776561741-1417001333-500MUTEX.DefaultS-1-5-21-515967899-776561741-1417001333-500

3.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office

2010)

3.2.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Attempted to determine public IP address via IP-checking website A system's client IP address within a network segment differs from its public IP address as seen from the network as a whole. Malware often queries a system's public IP address for a variety of reasons, including geolocation and evasion of known honeypots.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Enumerated running processes Malware often enumerates running processes before injecting malicious code into them.	
Modified Portable Executable image sections at runtime Portable Executable images contain sections with different access and execution permissions. These sections are built statically during compilation, and runtime modifications indicate binary obfuscation techniques.	

3.2.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
ipinfo.io	NS	ns-2012.awsdns-59.co.uk
ipinfo.io	A	216.239.36.21
ipinfo.io	NS	ns-348.awsdns-43.com
ipinfo.io	A	216.239.32.21
ipinfo.io	NS	ns-1247.awsdns-27.org
ipinfo.io	NS	ns-595.awsdns-10.net
ipinfo.io	A	216.239.34.21
ipinfo.io	A	216.239.38.21

HTTP Requests

HTTP Method	URL	User-Agent
GET	ipinfo.io/json	Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)

Connections

Host	Port	Protocol	Country

216.239.36.21	80	TCP	US

3.2.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

Process Activity

Child Process	Action
"C:\Users\ADMINI~1\AppData\Local\Temp\is-NGMIS.tmp\yrmsacifh.tmp" /SL5="$C014E,42518203,401920,C:\Users\Administrator\sample.exe"	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\ADMINI~1\AppData\Local\Temp\is-NGMIS.tmp\yrmsacifh.tmp	Create	1863168	exe	md5:d11b29425b3784cbcd42683ecd49bce3 sha1:d137b656e1e19d2400b60be2117c158d9e1c3090 sha256:7c2e6051378c52ac55cec1bf4a13601fcd51828db64e02c2e61e2345bc50f52d

Process Name - yrmsacifh.tmp

(command: "C:\Users\ADMINI~1\AppData\Local\Temp\is-NGMIS.tmp\yrmsacifh.tmp" /SL5="$C014E,42518203,401920,C:\Users\Administrator\sample.exe")

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\ADMINI~1\AppData\Local\Temp\Setup Log 2020-03-27 #001.txt	Create	3567	text	md5:59170e2a33e9b1285e57a6aa50a8a278 sha1:4c2bb7d97ba42f7d24aaeab416406a4abac652d7 sha256:74117bf4234e4e6a29af3c3673fc8b26e1bec5b5858a9dd33017a8c8a9e3ae33
C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp_isetup_setup64.tmp	Create	6144	exe64	md5:e4211d6d009757c078a9fac7ff4f03d4 sha1:019cd56ba687d39d12d4b13991c9a42ea6ba03da sha256:388a796580234efc95f3b1c70ad4cb44bfddc7ba0f9203bf4902b9929b136f95
C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp_isetup_iscrypt.dll	Create	2560	dll	md5:a69559718ab506675e907fe49deb71e9 sha1:bc8f404ffdb1960b50c12ff9413c893b56f2e36f sha256:2f6294f9aa09f59a574b5dcd33be54e16b39377984f3d5658cda44950fa0f8fc

C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\klcp_detect.dll	Create	79872	dll	md5:b4177c626953ba1095f1286c2e8421ea sha1:2b97124bfdd23f367a01d7f232f6520d3c28db45 sha256:4a8e9131335d41030583a2a6d193f235dd0b19a5086ea98d6b60618874083257
C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\klcp_detect2.dll	Create	157184	dll	md5:e1d9c0fadc965425fa7f091cd0c00109 sha1:3ede5ab647998c419d4cef927a2c6f44322547b8 sha256:3b9b9b540668ab5a8b6b7bfd23dc1009856b963db07a9fbcdc2ed2553bf4dba1
C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\mpc_logo.bmp	Create	65590	unknown	md5:565517c2f0973264e9376daa187c22da sha1:42f4a8b63e6a39677696e7668e68332 39b49d0e49 sha256:88d7b54d7a2b0f31b649a67de13ff690b005df1304c5e5e3ac9512c999263c64

Registry Activity

Registry Key	Value	Action
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000		Create
HKEY_LOCAL_MACHINE\Software\KLCodecPack		Create
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\MediaResources\DirectSound\Speaker Configuration\Speaker Configuration	4	Set
\REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\Owner	NULL	Set
\REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\SessionHash	NULL	Set
\REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\Sequence	1	Set
\REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\RegFiles0000	NULL	Set
\REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\RegFilesHash	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KLCodecPack\LastInstallRun	1585376641	Set

Created Mutexes

Mutex Name
klcp_setup_mutex
Local\DirectSound DllMain mutex (0x00000868)
Local__DDrawExclMode__
Local__DDrawCheckExclMode__
DirectSound Administrator shared thread array (lock)
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511

Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

Event Timeline

1	Created Process C:\Users\Administrator\sample.exe
2	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-NGMIS.tmp\yrmsacifh.tmp
3	Created Process "C:\Users\ADMINI~1\AppData\Local\Temp\is-NGMIS.tmp\yrmsacifh.tmp" /SL5="$C014E,42518203,401920,C:\Users\Administrator\sample.exe"
4	Created file C:\Users\ADMINI~1\AppData\Local\Temp\Setup Log 2020-03-27 #001.txt
5	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp_isetup_setup64.tmp
6	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp_isetup_iscrypt.dll
7	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\klcp_detect.dll
8	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\klcp_detect2.dll
9	Created mutex klcp_setup_mutex
10	Created mutex Local\DirectSound DllMain mutex (0x00000868)
11	Created mutex Local__DDrawExclMode__
12	Created mutex Local__DDrawCheckExclMode__
13	Created mutex DirectSound Administrator shared thread array (lock)
14	Set key \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\MediaResources\DirectSound\Speaker Configuration\Speaker Configuration to value 4
15	Set key \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\MediaResources\DirectSound\Speaker Configuration\Speaker Configuration to value 4
16	Created mutex Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
17	Set key \REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\Owner to value NULL
18	Set key \REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\SessionHash to value NULL
19	Created mutex Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
20	Set key \REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\Sequence to value 1
21	Set key \REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\RegFiles0000 to value NULL
22	Set key \REGISTRY\USER\S-1-5-21-843043956-3771856219-1177494106-500\Software\Microsoft\RestartManager\Session0000\RegFilesHash to value NULL
23	Set key \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KLCodecPack\LastInstallRun to value 1585376641
24	Created file C:\Users\ADMINI~1\AppData\Local\Temp\is-O0OG2.tmp\mpc_logo.bmp