DYNAMIC ANALYSIS REPORT

#11158857

MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe**
ID	#5295845
MD5	223eff1610b432a1f1aa06c60bd7b9a6
SHA1	14177730443c65aefeeda3162b324fdedf9cf9e0
SHA256	006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
File Size	178.50 KB
Report Created	2022-09-02 02:05 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (5 rules, 109 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 1934 files by appending the extension ".play".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
1/5	Hide Tracks	Changes folder appearance	6	-
	• (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\$Recycle.Bin\S-1-5-18". • (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000". • (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\Program Files\Common Files\microsoft shared\Stationery". • (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\Program Files". • (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Stationery". • (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe changes the appearance of folder "\\?\C:\Program Files (x86)".			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\F5u84D9.bmp".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\F5u84D9.bmp.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\gCH3TZQDDk2j9.png".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\gCH3TZQDDk2j9.png.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\Filters\VISFILT.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\en-us\oregres.dll.mui".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\en-us\oregres.dll.mui.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLMF.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXEV.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXEV.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLMF.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\Filters\VISFILT.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\VSTO\vstoee100.tlb".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\VSTO\vstoee100.tlb.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\rdCuc5FgRBkMF64Lt.png".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\rdCuc5FgRBkMF64Lt.png.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\VSTO\vstoee90.tlb".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\VSTO\vstoee90.tlb.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\desktop.ini".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\desktop.ini.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Internet Explorer\SIGNUP\install.ins".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Internet Explorer\SIGNUP\install.ins.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\MAPISHELLR.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\BHOINTL.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\MAPISHELLR.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\BHOINTL.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File A.txt".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File A.txt.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File B.txt".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\MAPISHELL.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\IEAWSDC.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\Custom.propdesc".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\Custom.propdesc.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentlogon.xml".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentlogon.xml.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentfallback.xml".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\officeinventoryagentfallback.xml.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\1033\Mso Example Intl Setup File B.txt.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\MAPISHELL.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\IEAWSDC.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\NAMEEXT.DLL".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\NAMEEXT.DLL.PLAY".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-manifest.ini".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote-PipelineConfig.xml".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft Office\Office16\OneNote\SendToOneNote.ini".
- (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe modifies "\\?\C:\Program Files\Microsoft

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe resolves 4470 API functions by name.			

Mitre ATT&CK Matrix

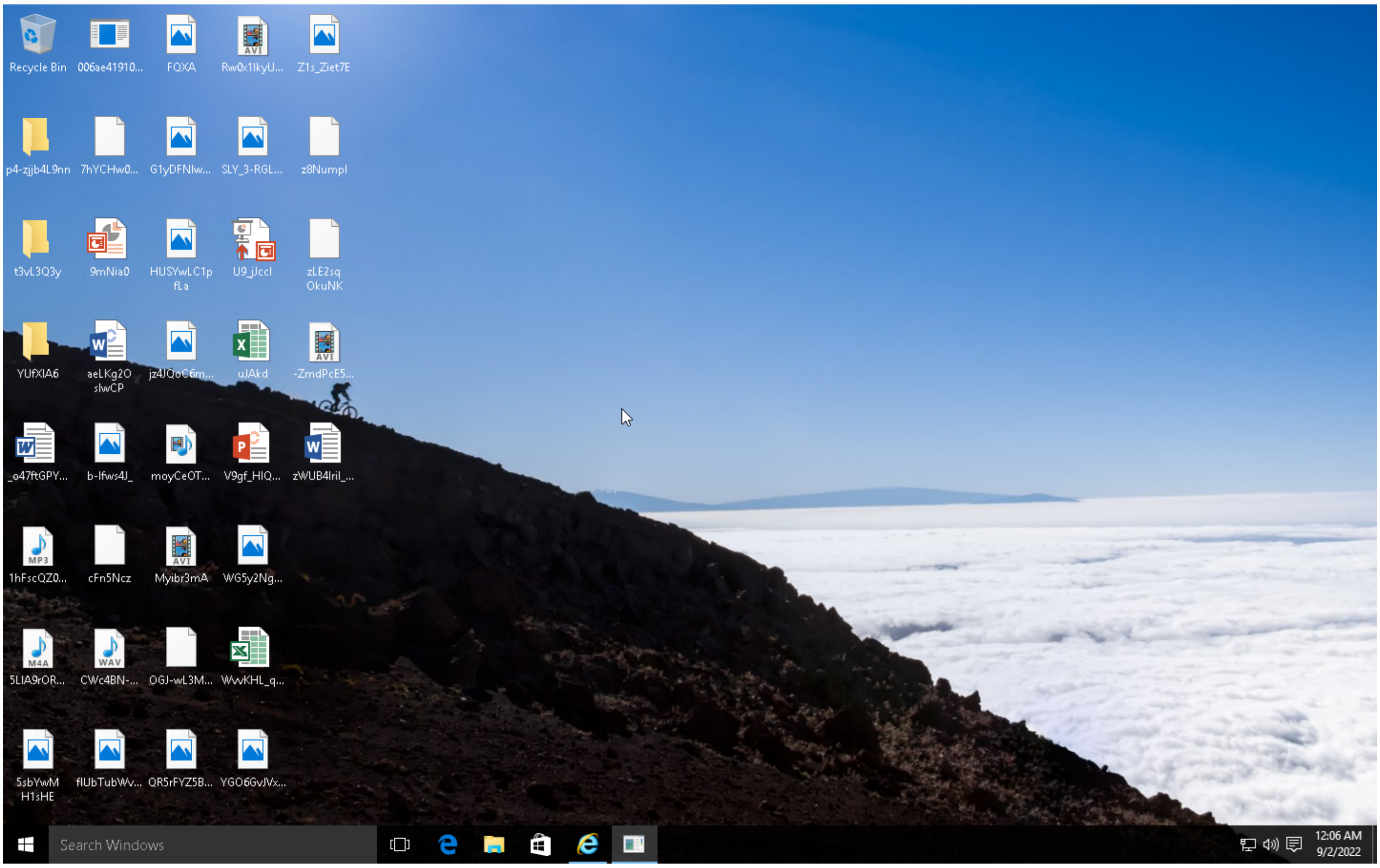
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1036 Masquerading							#T1486 Data Encrypted for Impact
				#T1045 Software Packing							

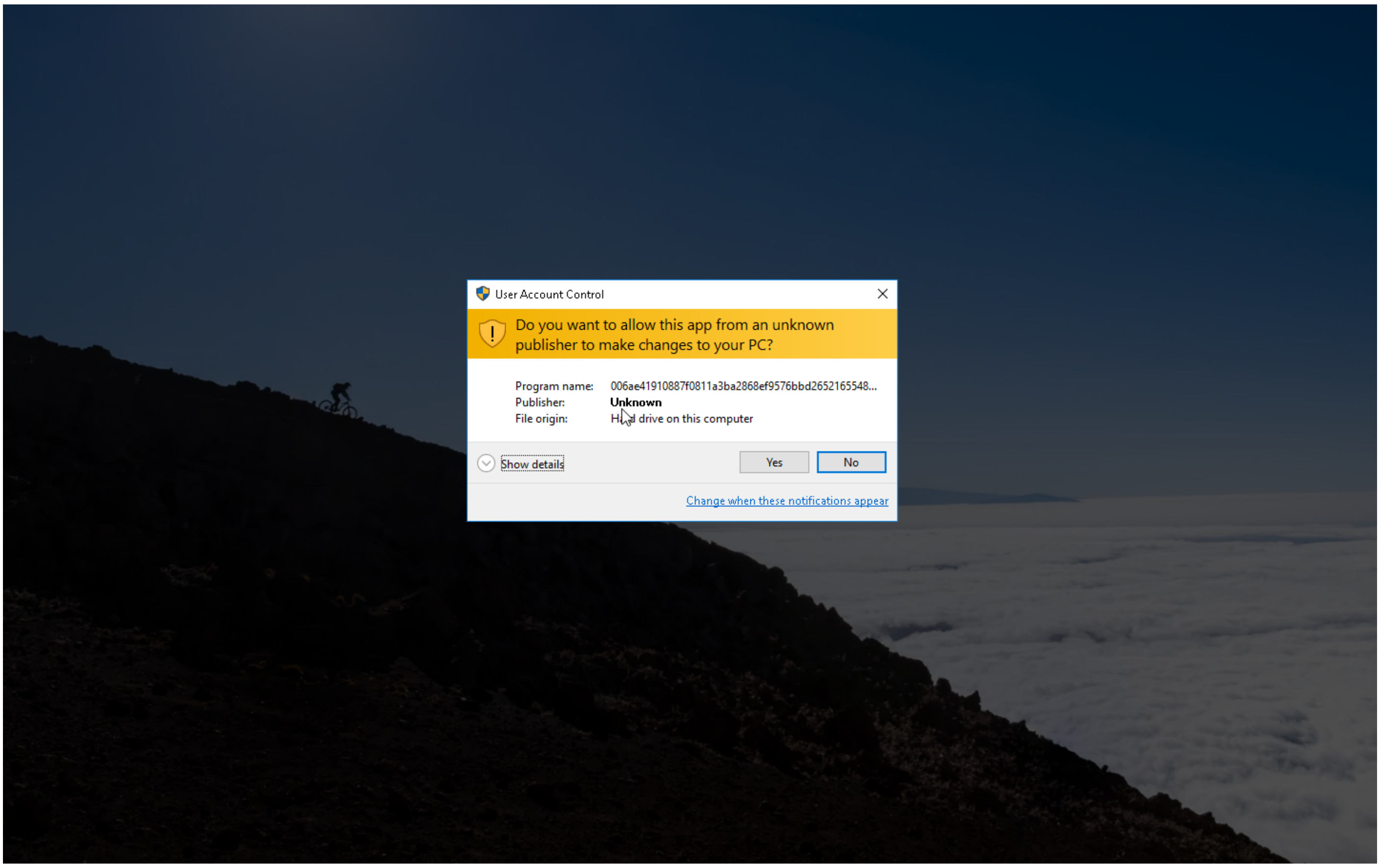
Sample Information

ID	#5295845
MD5	223eff1610b432a1f1aa06c60bd7b9a6
SHA1	14177730443c65aefeeda3162b324fdedf9cf9e0
SHA256	006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55
SSDeep	3072:Yrl2uRkddO+iR7OZOQ+dzeIP9mwUGU3l2bxW1/9JnOC/fhKJ2hXh3lmG:22uyqOh2g8U12K9dtEWx17
ImpHash	bfaffd974eb97f13ae5b4b98aa20c81e
File Name	006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe
File Size	178.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-09-02 02:05 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0

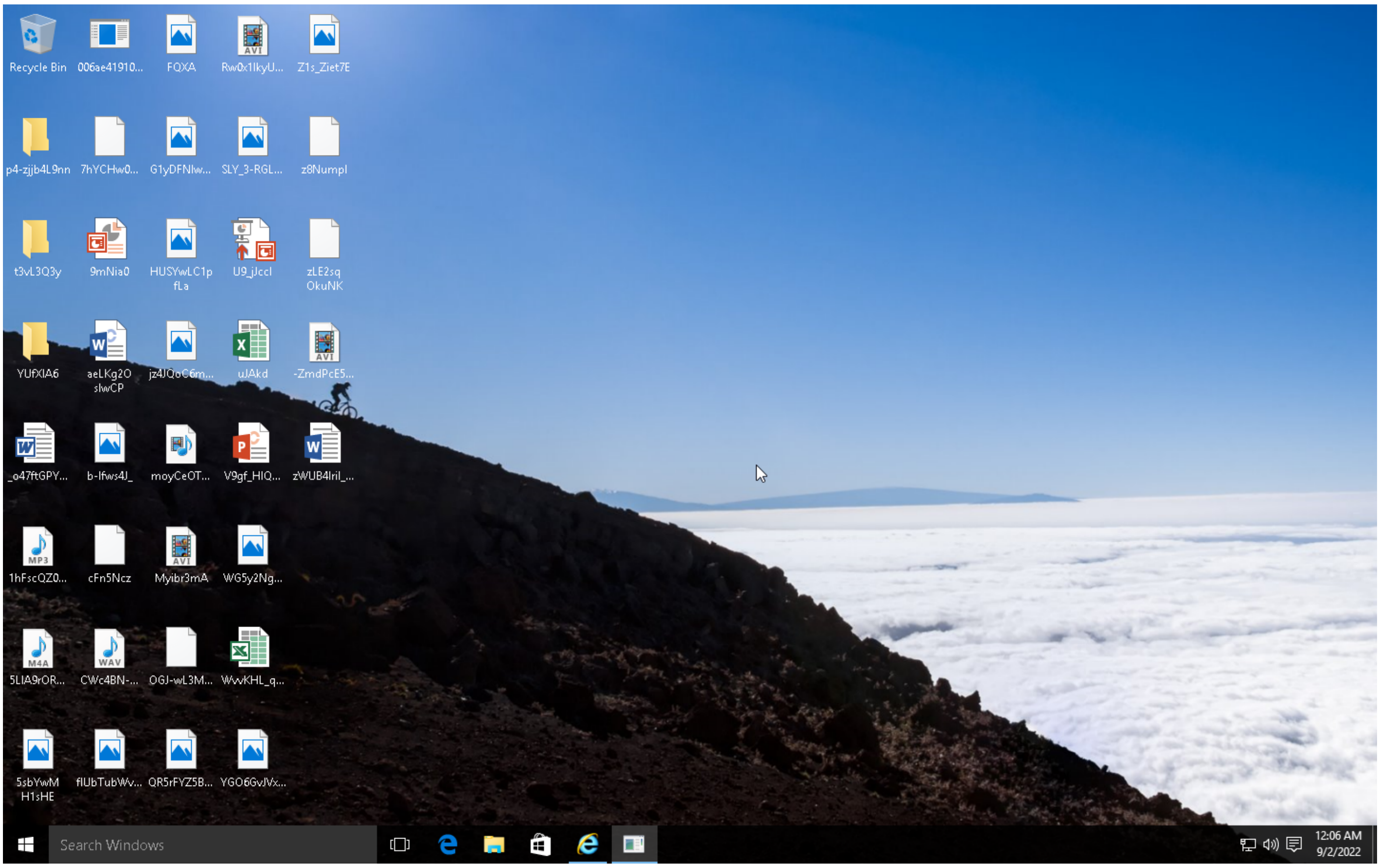


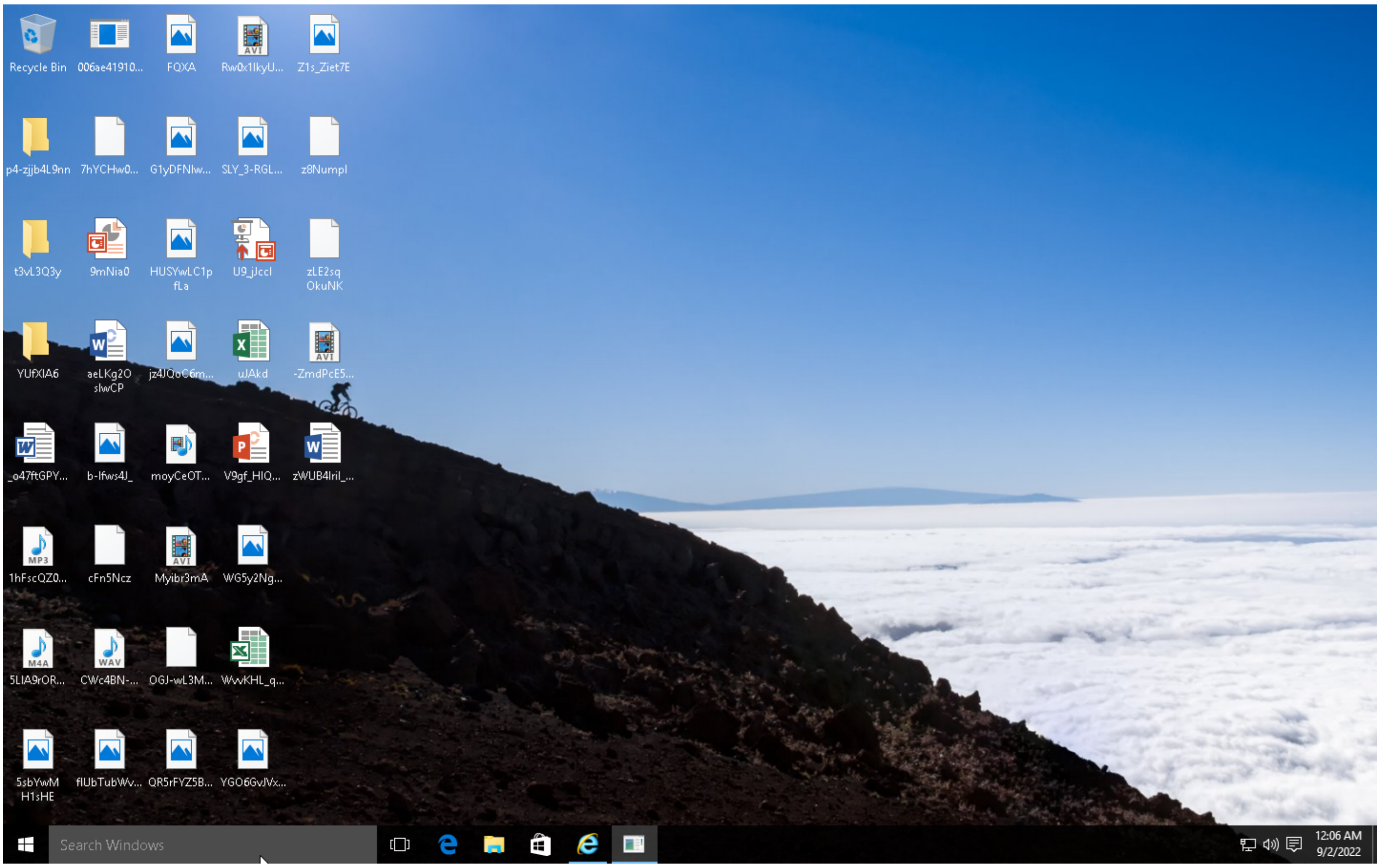


User Account Control

Do you want to allow this app from an unknown publisher to make changes to your PC?

Program name: 006ae41910887f0811a3ba2868ef9576bbd2652165548...
Publisher: **Unknown**
File origin: Hard drive on this computer


Recycle Bin
006ae41910...
FQXA
Rw0x1IkyU...
Z1s_Ziet7E
p4-zjjb4L9nn
7hYCHw0...
G1yDFNlw...
SLY_3-RGL...
z8Numpl
t3vL3Q3y
9mNia0
HUSYwLC1p fLa
U9_jJccl
zLE2sq OkuNK
YUfXIA6
aeLKg2O slwCP
jz4JQoC6m...
uJAkd
-ZmdPcE5...
_o47ftGPY...
b-Ifws4J_
moyCeOT...
V9gf_HIQ...
zWUB4lril_...
1hFscQZ0...
cFn5Ncz
Myibr3mA
WG5y2Ng...
5LIA9rOR...
CWc4BN-...
OGJ-wL3M...
WvKHL_q...
5sbYwM H1sHE
fIUbTubWv...
QR5rFYZ5B...
YGO6GvJVx...
Search Windows
12:06 AM
9/2/2022


Recycle Bin
006ae41910...
FQXA
Rw0x1IkyU...
Z1s_Ziet7E
p4-zjjb4L9nn
7hYCHw0...
G1yDFNlw...
SLY_3-RGL...
z8Numpl
t3vL3Q3y
9mNia0
HUSYwLC1p fLa
U9_jJccl
zLE2sq OkuNK
YUfXIA6
aeLKg2O slwCP
jz4JQoC6m...
uJAkd
-ZmdPcE5...
_o47ftGPY...
b-Ifws4J_
moyCeOT...
V9gf_HIQ...
zWUB4lril_...
1hFscQZ0...
cFn5Ncz
Myibr3mA
WG5y2Ng...
5LIA9rOR...
CWc4BN-...
OGJ-wL3M...
WvKHL_q...
5sbYwM H1sHE
fIUbTubWv...
QR5rFYZ5B...
YGO6GvJVx...
Search Windows
12:06 AM
9/2/2022

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

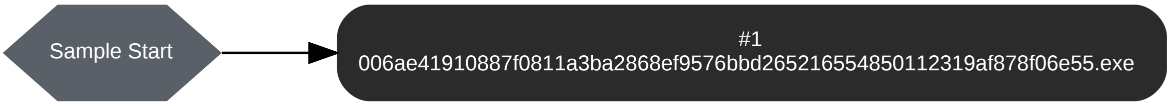
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph


Sample Start
#1
006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe

Process #1: 006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 67351, Reason: Analysis Target
Unmonitor End Time	End Time: 318336, Reason: Terminated by timeout
Monitor duration	250.99s
Return Code	Unknown
PID	4932
Parent PID	1972
Bitness	32 Bit

Dropped Files (2395)

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	3.07 KB	751d0a84c0393a4f060263d9158ead74a1cf1bda5c1117e5a108cdd025da04db	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.PLAY	16.38 KB	85962c392645215484a0db98955feca8f9ad4085e7f303c59ad62c94a5225ae8	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.cab.play	10240.00 KB	848a5dc005d6a8f69bb2f2ae1e39914cba1e03abb76a890fc702f9aab1ad7823	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	6.98 KB	9f527b0a4c8b287e492db23d2f5d92134fa7fae0d70f7050158099931e5f0123	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.cab.PLAY	10240.00 KB	195e640779176ba554b54b8c78856b0e796f34c3df3b257629913a5b6b8350dd	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST.PLAY	11.55 KB	b2bb4bc375fdcd61cb8519e7686171d4c28fbe0f00111ae27c5c4853e46d94c7	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.cab.PLAY	10240.00 KB	c8a9d80ce8211bdcd3bde2c97394e3511f7da9a2a87b0679d8ea58334da06acb	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.PLAY	6.20 KB	03197a1d612cedfd9e18d3dabf04cf788a93074dbb8ad9f77fb19c9a5d5da5ed	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.PLAY	3821.02 KB	eab30a0381ca2d118984314495862c287d9617836218361efd33d16da799ebd4	✖
c:\program files\common files\microsoft shared\office16\msoxmlmf.dll.play	65.24 KB	b2e3fa55b4123ca442be8845e4b45ed7d67e3660f737b9191f8e8536d6ff50c4	✖
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.PLAY	2.23 KB	7be990b0a2d46c77c725846b91acb397788dad5fa803efc2ec4053ea85c0c49a	✖
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	3.45 KB	9f179805ba775dec55834823ee101123a4f8a9b32e7a15464c462f7fad7cf818	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.PLAY	2.66 KB	efd5a293d9c825305bc1782c7778b0c081681759d003a9dfa91a0ff29495ce56	✖
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.PLAY	853.55 KB	631a0f043c655bb8c9966d11058d6436718f3b862cbd6a63b8e7e72fd32ec502	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.xml.play	3.82 KB	0962574a29b38f87530285988c9cf7a5814618d88b8525ceea8a665792546f64	✖

File Name	File Size	SHA256	YARA Match
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.xml.play	2.57 KB	db6e275960c380dbaa3c8d68c76df650d74f0461ec737cbcb8d98939f2daa136	✖
c:\program files\common files\gch3tzqddk2j9.png.play	90.90 KB	842595ba217210e5af77b679f9ca265a4c670bcd438634aad9cd455b0409b7e2	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.PLAY	2.68 KB	5bced65dd2f9e2d1d8956a2c93bbfcd7a4cb260ea7617fe9d070832e1fd3ab4c	✖
c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\pptlr.cab.play	6163.29 KB	295c587796bc47e301bdf4dff8aeb364ee89af3622787c3e6d411db298558ef4	✖
c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\setup.xml.play	3.48 KB	2e2ac90cef5a3e09ec024e1f227f2599082e24c12c2d9795c0b478dcb460b274	✖
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab.PLAY	17.46 KB	dbd08c545ade5a130622fac9a3efa536feb9e39a1a08e7833334e8e877e92f1f	✖
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\pss10r.chm.play	15.30 KB	4a1454a15d33b4a584fa3eded9607047dff382b172070fe36ef1021057c16701	✖
\\?\C:\ReadMe.txt	31 bytes	6e55acc025ea4888fdf070a1707b6e04a509b24772e81d64595ea6b2848dd71f	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.PLAY	10240.00 KB	e301e533db841e8ab4900ae5b692e6555bf430c7adf10428566f1b8e84fb1d8f	✖
c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\office64muiset.xml.play	2.05 KB	f197658d1de8faa7078a04502d847b03c4efec278cf0cbcbb68707d069f18631	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.xml.play	3.10 KB	c08fd299834c03e684df7c71ded90080ee74d6541f37de60fdb566d75c6a844c	✖
c:\$recycle.bin\s-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.play	1.18 KB	a65aa7d4862a3891592dc3862a7ff6bfc95af82f3290f1e54baaace5e5205c29	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.PLAY	2.79 KB	fbf232ae291df6927fd97684c6594818d32a4e68e8a36dfb8e81a3e213b9399b	✖
c:\$recycle.bin\s-1-5-18\desktop.ini.play	1.18 KB	306f54d3f4ea692516d14c44569ce62bba7a672db784038752fbac69286e5db6	✖
\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.PLAY	3916.27 KB	95233b19cb5bec677e2bc47aaef1aa33bf5083f0ad82610c1cbf487a6b3f25cc	✖
c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.xml.play	2.15 KB	b2c2eadd8dcde0eb625675a3d30b407edbfb03aa57e798521a9eaba707a3aec4	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.PLAY	2.05 KB	61a075220dbcd1959a7703418785cec14bbe059e0193fd2fa261c43678b5991e	✖
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\setup.xml.play	3.57 KB	efcbad2f97d4d2d169fad7543057ba3ac09b8dcfbdaca876acc33f9f5759f830	✖
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\acclr.cab.play	5272.60 KB	b1be40a9bb3aa6b6c2230221e1ff3750cdca213b4dca4e8c28a725fda4a5f6d0	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\setup.xml.play	3.76 KB	07794eb0a466230d47f80385c58987e65d12287b20412b60f87287eeeac01b1c	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	9.34 KB	2c5422d05a3c33316b1cbc3834abf4394ef7650c3e1520e4db3de093c6d4e7c5	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.PLAY	2.66 KB	194dfa1bdc72e214811480968d126e916ab81395aa3a90848e78b24eae5f6a52	✖
c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.xml.play	2.15 KB	bbc161515deac06d175f0eaa11951ae4129a06e0664a7bf691620715d138ced6	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.PLAY	2.24 KB	70e9bb98cd959130e903e5f6f014345d01ab856d190c625b4fdb8e0de3455db1	✖
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\accessmui.xml.play	2.46 KB	d6b40e1af4aa821a69a78daf0c57ae01d97cff1e61ea7b1b63e4dda9e4ed92b7	✖
c:\program files\common files\microsoft shared\office16\en-us\oregres.dll.mui.play	16.55 KB	d893eeb2f0bbc3ab2fb9f879642024eb5b9dfdea4534c5561263f678aeef9de9	✖

File Name	File Size	SHA256	YARA Match
c:\program files\common files\microsoft shared\office16\msoxmled.exe.play	217.21 KB	dda3b564a8d2c807637e65480ab2468395b6518c841be68c4d653fc17d604a1e	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.play	9844.55 KB	1d8ed236735a79e5fb75314a15f7b4aa6a6176ae6deac3aec37e8c1989145461	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.xml.play	2.68 KB	99c2ea43a425113849e26fcda1f1e258609119d6986e4e94051f5df2461e5247	✖
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	3.04 KB	8ecc49b6a076c2eb81c3fd44d22894c1e0ba0c5886cf3245c63ceefafb66b488	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.xml.play	5.93 KB	2f4af3f5f6e7a9008471d5a66b173baa9038a27f973c39fe440f6bc9f83500be	✖
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.PLAY	2.48 KB	e81993c5c29e0644b18e678e8a376e1916036453eaf1a8813ff3cf888063f6e1	✖
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\branding.xml.play	329.48 KB	420e692601f39e66882b489b9369135f8ae09dc337f7d2cda7e2ef4d318fcfdf	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.PLAY	2.82 KB	1b3de26f4c8887f57204454b2f86688ada67f8ee5c446f3e7396137a43972a3d	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\setup.xml.play	4.82 KB	82d69674c3184837ef8bbca502c71bf6611f39990028bc45496a7d10106808a8	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propluswww.xml.play	17.76 KB	0d355be48fab1c7d72da1105ea6621cc60e4c4c2db1bae378fa034d966c5a0f5	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	3.16 KB	7a5deee2cbd340ecd8df7e54d4e1bf4ee2bcbd9c5e5f0807787ea1a62a762d31	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.PLAY	10240.00 KB	f3d6e14c2935e53f3ee1cddda22250744628e191e394703ed10089af9f28bd92	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.PLAY	10240.00 KB	c9883f3ef4c5c85886dfc63a274553cd7771f8ec0a4746398d32fed83a357b6f	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\pkeyconfig-office.xrm-ms.play	577.73 KB	2ef4fba05f7e8f99a103a8d2fbc9aa239b9c14e25869020beef91a12acf7f3dd	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	2.80 KB	11977695767f6edb9d401cd9f32208e6209362045f6517cdac1d6e77a1e4d7c8	✖
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.cab.play	627.60 KB	05839090afa2356fe49a529a2a640dee92700d89fe4a13de6992c5032cdc9d98	✖
c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publr.cab.play	3479.21 KB	929dea4a27295d38a4ba65eda6c91b736f02e632e31a5c7ad34e2bcc69e8e68f	✖
c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\osmuxmui.cab.play	4132.59 KB	5909f3657a2ccc46eef006c5efec4675aa06d8352d1417e6f7ed2510ad327f0e	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.PLAY	329.48 KB	160fad43a4846b4991d699bb79940cdbac5d2ef6deb9ebe011d282ca5f1917af	✖
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\accessmuiset.xml.play	2.05 KB	a64f901f3ea8dfdf4bd85d0f927511d351daa719f0d076f05177abb29979f424	✖
c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\setup.xml.play	4.10 KB	3ad13e13da459892fe073f51158301a14a3ab00972390c141e562f7da2d2fb54	✖
\\?\C:\Program Files\Common Files\F5u84D9.bmp.PLAY	78.99 KB	0c51680a0325fc90246b0c1846462f63d3adf8b028cec36a614aa0072bac0aaf	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	2.80 KB	881a3839658db01375cb28f7bbf2fa1035c82a633b49f50f7050267e4d408222	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.xml.play	2.05 KB	35c20bc1abc0dcdcfc429529dcc38a07929dcb21cd81d0521458d64234197187	✖
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\setup.xml.play	2.82 KB	f39621b17715ea44751e70fd1864c7a7b3fb8a764a83b8693a67ac34cf076eff	✖
\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	2.70 KB	8a5ed95cdece04bcb8557a8353ba78506136e9cb78ea7eb4476d5f00fda059c3	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\BOOTSECT.BAK.PLAY	9.05 KB	54219b2d1b3854ec3408384154156a6c2250ff4f9ea5ae363e04fa5e22e81e6f	✖
c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\lyncmui.cab.play	2548.51 KB	4a019144b62cd8aeab5838cd65d61f5c5168e2ddc06f7a9fc7b17529c4fce6d0	✖
c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\lyncmui.xml.play	2.24 KB	821bbc0fef3974c93a77e768775a5fe5b2971a426c634a8f1bf0d7406f4ef379	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm.PLAY	81.90 KB	9f3550df2a155b765bb45138208a9583f4ed54fb3347575284ec0e1f4f8d252f	✖
\\?\C:\Program Files\Common Files\microsoft shared\Filters\VISFILT.DLL.PLAY	5957.76 KB	3a16be50f5a5165e6a8f60df8ac78f2cf288a06eb668bf1aa9d9500a46ded5ca	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab.PLAY	10240.00 KB	18cb7162956589ec12aeadd06a027cf157944b7488523cf7b5e83bf48aadf339	✖
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.PLAY	2.91 KB	6f111d690716247d9ce9b9204806d9e1637d4407d322e390e97072efb955b996	✖
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab.PLAY	2013.21 KB	a14d3ab03578ceca7baf8746ebbe3675cdc46062f88a384e9a43c8fa0e5a9175	✖
\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini.PLAY	1.68 KB	55daccef353405cea13c5788d5bc04be460796c68d2bccd9f3e6de4168abbc50	✖
c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.play	5635.40 KB	7e7dc686a11e17b9a331832b2ef499a77a7281821b172f533e8097b3e877d1cd	✖
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	2.65 KB	b53f10229a068461c30ccd6e2e98d66fd16dd830a2e317d0a1d57d2fe967a105	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\setup.xml.play	28.18 KB	daae6a0b3b114d4217580f289161705f1ad82320a57e4d69a84418dd4b2f7612	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab.PLAY	10240.00 KB	80c1dd82510d1b437178ec1c46333206fcf367e4901638ace4d669e0e5643123	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\PROFILE\THMBNAIL.PNG	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH02298_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Smart Tag\FBIBLIO.DLL	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA01130_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BS01080_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01772_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\vba\vba7.1\vbeui.dll.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01145_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BL00152_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0107042.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH00084_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341534.jpg.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\themes16\arctic\arctic.elm.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\AXIS\PREVIEW.GIF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH01013_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0105530.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\COMPASS\PREVIEW.GIF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01176_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0152590.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0153305.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BL00648_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\na01358_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\themes16\layers\preview.gif.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\an04225_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\REFINED\REFINED.ELM	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\na02356_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH01923_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0187825.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02058u.bmp.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\TRANSLAT\MSB1CORE.DLL.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\BLUEPRNT\THMBNAIL.PNG	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0093905.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\dd00255_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0105250.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0099181.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA7.1\1033\VBENDF98.CHM.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0105526.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\RMNSQUE\PREVIEW.GIF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\Cartridges\as80.xsl	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099173.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PE06049_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\na02451_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0164153.jpg.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\clipart\pub60cor\ph03425i.jpg.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\themes16\compass\thmbnail.png.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02208u.bmp.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\vba\vba7.1\1033\fm20.chm.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\DD01181_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0182902.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0239935.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\bd08773_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0285782.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\common files\microsoft shared\themes16\cascade\thmbnail.png.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0101864.BMP	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0101867.BMP	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099147.JPG.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\AFTRNOON\AFTRNOON.INF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BS00076_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\ICE\THMBNAIL.PNG	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0172193.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AN01060_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0188667.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0152702.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\SKY\PREVIEW.GIF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BL00524_.WMF.PLAY	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\j0099168.jpg.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files (x86)\microsoft office\clipart\pub60cor\fd01084_.wmf.play	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH00276_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\ED00019_.WMF	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Reduced dataset

Host Behavior

Type	Count
Module	5007
File	17540
Environment	1
System	52
-	1706

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55	C:\Users\RDhJ0CNFevzX\Desktop\006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe	Sample File	178.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
751d0a84c0393a4f060263d9158ead74a1cf1bda5c1117e5a108cdd025da04db	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	3.07 KB	application/octet-stream	Access, Create, Write	CLEAN
85962c392645215484a0db98955feca8f9ad4085e7f303c59ad62c94a5225ae8	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\offsetlr.cab.play	Dropped File	16.38 KB	application/octet-stream	Access, Create, Write	CLEAN
848a5dc005d6a8f69bb2f2ae1e39914cba1e03abb76a890fc702f9aab1ad7823	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.cab.play, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.cab.PLAY	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
9f527b0a4c8b287e492db23d2f5d92134fa7fae0d70f7050158099931e5f0123	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	6.98 KB	application/octet-stream	Access, Create, Write	CLEAN
195e640779176ba554b54b8c78856b0e796f34c3df3b257629913a5b6b8350dd	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.cab.PLAY, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
b2bb4bc375fdcd61cb8519e7686171d4c28fbe0f00111ae27c5c4853e46d94c7	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\shellui.mst.play	Dropped File	11.55 KB	application/octet-stream	Access, Create, Write	CLEAN
c8a9d80ce8211bdcd3bde2c97394e3511f7da9a2a87b0679d8ea58334da06acb	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.cab.PLAY, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.cab.play	Dropped File	10240.00 KB	audio/x-mp4a-latm	Access, Create, Write	CLEAN
03197a1d612cedfd9e18d3dabf04cf788a93074dbb8ad9f77fb19c9a5d5da5ed	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemui.xml.play	Dropped File	6.20 KB	application/octet-stream	Access, Create, Write	CLEAN
eab30a0381ca2d118984314495862c287d9617836218361efd33d16da799ebd4	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.PLAY, c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\inflr.cab.play	Dropped File	3821.02 KB	application/octet-stream	Access, Create, Write	CLEAN
b2e3fa55b4123ca442be8845e4b45ed7d67e3660f737b9191f8e8536d6ff50c4	c:\program files\common files\microsoft shared\office16\msoxmlmf.dll.play, \\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLMF.DLL.PLAY	Dropped File	65.24 KB	application/octet-stream	Access, Create, Write	CLEAN
7be990b0a2d46c77c725846b91acb397788dad5fa803efc2ec4053ea85c0c49a	\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.PLAY, c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.xml.play	Dropped File	2.23 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9f179805ba775dec55834823ee101123a4f8a9b32e7a15464c462f7fad7cf818	\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	3.45 KB	application/octet-stream	Access, Create, Write	CLEAN
efd5a293d9c825305bc1782c7778b0c081681759d003a9dfa91a0ff29495ce56	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.PLAY, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.xml.play	Dropped File	2.66 KB	application/octet-stream	Access, Create, Write	CLEAN
631a0f043c655bb8c9966d11058d6436718f3b862cbd6a63b8e7e72fd32ec502	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.PLAY, c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovelr.cab.play	Dropped File	853.55 KB	application/octet-stream	Access, Create, Write	CLEAN
0962574a29b38f87530285988c9cf7a5814618d88b8525ceea8a665792546f64	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.xml.play, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.PLAY	Dropped File	3.82 KB	application/octet-stream	Access, Create, Write	CLEAN
db6e275960c380dbaa3c8d68c76df650d74f0461ec737cbcb8d98939f2daa136	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.xml.play, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.PLAY	Dropped File	2.57 KB	application/octet-stream	Access, Create, Write	CLEAN
842595ba217210e5af77b679f9ca265a4c670bcd438634aad9cd455b0409b7e2	c:\program files\common files\gch3tzqddk2j9.png.play, \\?\C:\Program Files\Common Files\gCH3TZQDDk2j9.png.PLAY	Dropped File	90.90 KB	application/octet-stream	Access, Create, Write	CLEAN
5bced65dd2f9e2d1d8956a2c93bbfcd7a4cb260ea7617fe9d070832e1fd3ab4c	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.PLAY, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.xml.play	Dropped File	2.68 KB	application/octet-stream	Access, Create, Write	CLEAN
295c587796bc47e301bdf4dff8aeb364ee89af3622787c3e6d411db298558ef4	c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\pptlr.cab.play, \\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.PLAY	Dropped File	6163.29 KB	application/octet-stream	Access, Create, Write	CLEAN
c360e112441ba289abf78e14f6dc6b553b5b90a5a7b317e95f6c42ba6447d23f	\\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXEV.DLL, c:\program files\common files\microsoft shared\office16\msoxev.dll.play, \\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXEV.DLL.PLAY	Modified File	69.71 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2e2ac90cef5a3e09ec024e1f227f2599082e24c12c2d9795c0b478dcb460b274	c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	3.48 KB	application/octet-stream	Access, Create, Write	CLEAN
dbd08c545ade5a130622fac9a3efa536feb9e39a1a08e7833334e8e877e92f1f	\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab.PLAY, c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.cab.play	Dropped File	17.46 KB	application/octet-stream	Access, Create, Write	CLEAN
4a1454a15d33b4a584fa3eded9607047dff382b172070fe36ef1021057c16701	c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\pss10r.chm.play, \\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm.PLAY	Dropped File	15.30 KB	application/octet-stream	Access, Create, Write	CLEAN
6e55acc025ea4888fdf070a1707b6e04a509b24772e81d64595ea6b2848dd71f	\\?\C:\ReadMe.txt	Dropped File	31 bytes	text/plain	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e301e533db841e8ab4900ae5b692e6555bf430c7adf10428566f1b8e84fb1d8f	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.PLAY, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\owow64ww.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
f197658d1de8faa7078a04502d847b03c4efec278cf0cbcbb68707d069f18631	c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\office64muiset.xml.play, \\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml.PLAY	Dropped File	2.05 KB	application/octet-stream	Access, Create, Write	CLEAN
c08fd299834c03e684df7c71ded90080ee74d6541f37de60fdb566d75c6a844c	c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.xml.play, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.PLAY	Dropped File	3.10 KB	application/octet-stream	Access, Create, Write	CLEAN
a65aa7d4862a3891592dc3862a7ff6bfc95af82f3290f1e54baaace5e5205c29	c:\$recycle.bin\s-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.play, \\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.PLAY	Dropped File	1.18 KB	application/octet-stream	Access, Create, Write	CLEAN
fbf232ae291df6927fd97684c6594818d32a4e68e8a36dfb8e81a3e213b9399b	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.PLAY, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excelmui.xml.play	Dropped File	2.79 KB	application/octet-stream	Access, Create, Write	CLEAN
306f54d3f4ea692516d14c44569ce62bba7a672db784038752fbac69286e5db6	c:\$recycle.bin\s-1-5-18\desktop.ini.play, \\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini.PLAY	Dropped File	1.18 KB	application/octet-stream	Access, Create, Write	CLEAN
95233b19cb5bec677e2bc47aaef1aa33bf5083f0ad82610c1cbf487a6b3f25cc	\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.PLAY, c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlklr.cab.play	Dropped File	3916.27 KB	application/octet-stream	Access, Create, Write	CLEAN
b2c2eadd8dcde0eb625675a3d30b407edbfb03aa57e798521a9eaba707a3aec4	c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.xml.play, \\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.PLAY	Dropped File	2.15 KB	application/octet-stream	Access, Create, Write	CLEAN
61a075220dbcd1959a7703418785cec14bbe059e0193fd2fa261c43678b5991e	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemuiset.xml.play	Dropped File	2.05 KB	application/octet-stream	Access, Create, Write	CLEAN
efcbad2f97d4d2d169fad7543057ba3ac09b8dcfbdaca876acc33f9f5759f830	c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	3.57 KB	application/octet-stream	Access, Create, Write	CLEAN
b1be40a9bb3aa6b6c2230221e1ff3750cdca213b4dca4e8c28a725fda4a5f6d0	c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\acclr.cab.play, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccLR.cab.PLAY	Dropped File	5272.60 KB	application/octet-stream	Access, Create, Write	CLEAN
07794eb0a466230d47f80385c58987e65d12287b20412b60f87287eeeac01b1c	c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	3.76 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2c5422d05a3c33316b1cbc3834abf4394ef7650c3e1520e4db3de093c6d4e7c5	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	9.34 KB	application/octet-stream	Access, Create, Write	CLEAN
194dfa1bdc72e214811480968d126e916ab81395aa3a90848e78b24eae5f6a52	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml.PLAY, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.xml.play	Dropped File	2.66 KB	application/octet-stream	Access, Create, Write	CLEAN
bbc161515deac06d175f0eaa11951ae4129a06e0664a7bf691620715d138ced6	c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.xml.play, \\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.PLAY	Dropped File	2.15 KB	application/octet-stream	Access, Create, Write	CLEAN
70e9bb98cd959130e903e5f6f014345d01ab856d190c625b4fdb8e0de3455db1	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.PLAY, c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\infopathmui.xml.play	Dropped File	2.24 KB	application/octet-stream	Access, Create, Write	CLEAN
d6b40e1af4aa821a69a78daf0c57ae01d97cff1e61ea7b1b63e4dda9e4ed92b7	c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\accessmui.xml.play, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.xml.PLAY	Dropped File	2.46 KB	application/octet-stream	Access, Create, Write	CLEAN
d893eeb2f0bbc3ab2fb9f879642024eb5b9dfdea4534c5561263f678aeef9de9	c:\program files\common files\microsoft shared\office16\en-us\oregres.dll.mui.play, \\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\en-us\oregres.dll.mui.PLAY	Dropped File	16.55 KB	application/octet-stream	Access, Create, Write	CLEAN
dda3b564a8d2c807637e65480ab2468395b6518c841be68c4d653fc17d604a1e	c:\program files\common files\microsoft shared\office16\msoxmled.exe.play, \\?\C:\Program Files\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE.PLAY	Dropped File	217.21 KB	application/octet-stream	Access, Create, Write	CLEAN
1d8ed236735a79e5fb75314a15f7b4aa6a6176ae6deac3aec37e8c1989145461	c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.play, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.PLAY	Dropped File	9844.55 KB	application/octet-stream	Access, Create, Write	CLEAN
99c2ea43a425113849e26fcda1f1e258609119d6986e4e94051f5df2461e5247	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.xml.play, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.xml.PLAY	Dropped File	2.68 KB	application/octet-stream	Access, Create, Write	CLEAN
8ecc49b6a076c2eb81c3fd44d22894c1e0ba0c5886cf3245c63ceefafb66b488	\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	3.04 KB	application/octet-stream	Access, Create, Write	CLEAN
2f4af3f5f6e7a9008471d5a66b173baa9038a27f973c39fe440f6bc9f83500be	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.xml.play, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml.PLAY	Dropped File	5.93 KB	application/octet-stream	Access, Create, Write	CLEAN
e81993c5c29e0644b18e678e8a376e1916036453eaf1a8813ff3cf888063f6e1	\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.PLAY, c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\osmuxmui.xml.play	Dropped File	2.48 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
420e692601f39e66882b489b9369135f8ae09dc337f7d2cda7e2ef4d318fcfdf	c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\branding.xml.play, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.PLAY	Dropped File	329.48 KB	application/octet-stream	Access, Create, Write	CLEAN
1b3de26f4c8887f57204454b2f86688ada67f8ee5c446f3e7396137a43972a3d	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.PLAY, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onenotemui.xml.play	Dropped File	2.82 KB	application/octet-stream	Access, Create, Write	CLEAN
82d69674c3184837ef8bbca502c71bf6611f39990028bc45496a7d10106808a8	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	4.82 KB	application/octet-stream	Access, Create, Write	CLEAN
0d355be48fab1c7d72da1105ea6621cc60e4c4c2db1bae378fa034d966c5a0f5	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.xml.play, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml.PLAY	Dropped File	17.76 KB	application/octet-stream	Access, Create, Write	CLEAN
7a5deee2cbd340ecd8df7e54d4e1bf4ee2bcbd9c5e5f0807787ea1a62a762d31	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	3.16 KB	application/octet-stream	Access, Create, Write	CLEAN
f3d6e14c2935e53f3ee1cddda22250744628e191e394703ed10089af9f28bd92	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.PLAY, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
c9883f3ef4c5c85886dfc63a274553cd7771f8ec0a4746398d32fed83a357b6f	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.PLAY, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww2.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN
2ef4fba05f7e8f99a103a8d2fbc9aa239b9c14e25869020beef91a12acf7f3dd	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\pkeyconfig-office.xrm-ms.play, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.PLAY	Dropped File	577.73 KB	application/octet-stream	Access, Create, Write	CLEAN
11977695767f6edb9d401cd9f32208e6209362045f6517cdac1d6e77a1e4d7c8	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	2.80 KB	application/octet-stream	Access, Create, Write	CLEAN
05839090afa2356fe49a529a2a640dee92700d89fe4a13de6992c5032cdc9d98	c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.cab.play, \\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.PLAY	Dropped File	627.60 KB	application/octet-stream	Access, Create, Write	CLEAN
929dea4a27295d38a4ba65eda6c91b736f02e632e31a5c7ad34e2bcc69e8e68f	c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publr.cab.play, \\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.PLAY	Dropped File	3479.21 KB	application/octet-stream	Access, Create, Write	CLEAN
5909f3657a2ccc46eef006c5efec4675aa06d8352d1417e6f7ed2510ad327f0e	c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\osmuxmui.cab.play, \\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab.PLAY	Dropped File	4132.59 KB	application/x-dosexec	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
160fad43a4846b4991d699bb79940cdbac5d2ef6deb9ebe011d282ca5f1917af	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\branding.xml.play	Dropped File	329.48 KB	application/octet-stream	Access, Create, Write	CLEAN
a64f901f3ea8dfdf4bd85d0f927511d351daa719f0d076f05177abb29979f424	c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\accessmuiset.xml.play, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml.PLAY	Dropped File	2.05 KB	application/octet-stream	Access, Create, Write	CLEAN
3ad13e13da459892fe073f51158301a14a3ab00972390c141e562f7da2d2fb54	c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	4.10 KB	application/octet-stream	Access, Create, Write	CLEAN
0c51680a0325fc90246b0c1846462f63d3adf8b028cec36a614aa0072bac0aaf	\\?\C:\Program Files\Common Files\F5u84D9.bmp.PLAY, c:\program files\common files\f5u84d9.bmp.play	Dropped File	78.99 KB	application/octet-stream	Access, Create, Write	CLEAN
881a3839658db01375cb28f7bbf2fa1035c82a633b49f50f7050267e4d408222	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	2.80 KB	application/octet-stream	Access, Create, Write	CLEAN
35c20bc1abc0dcdcfc429529dcc38a07929dcb21cd81d0521458d64234197187	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.xml.play, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.PLAY	Dropped File	2.05 KB	application/octet-stream	Access, Create, Write	CLEAN
f39621b17715ea44751e70fd1864c7a7b3fb8a764a83b8693a67ac34cf076eff	c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	2.82 KB	application/octet-stream	Access, Create, Write	CLEAN
8a5ed95cdece04bcb8557a8353ba78506136e9cb78ea7eb4476d5f00fda059c3	\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	2.70 KB	application/octet-stream	Access, Create, Write	CLEAN
54219b2d1b3854ec3408384154156a6c2250ff4f9ea5ae363e04fa5e22e81e6f	\\?\C:\BOOTSECT.BAK.PLAY, c:\bootsect.bak.play	Dropped File	9.05 KB	application/octet-stream	Access, Create, Write	CLEAN
4a019144b62cd8aeab5838cd65d61f5c5168e2ddc06f7a9fc7b17529c4fce6d0	c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\lyncmui.cab.play, \\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab.PLAY	Dropped File	2548.51 KB	application/octet-stream	Access, Create, Write	CLEAN
821bbc0fef3974c93a77e768775a5fe5b2971a426c634a8f1bf0d7406f4ef379	c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\lyncmui.xml.play, \\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.PLAY	Dropped File	2.24 KB	application/octet-stream	Access, Create, Write	CLEAN
9f3550df2a155b765bb45138208a9583f4ed54fb3347575284ec0e1f4f8d252f	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\setup.chm.play	Dropped File	81.90 KB	application/octet-stream	Access, Create, Write	CLEAN
3a16be50f5a5165e6a8f60df8ac78f2cf288a06eb668bf1aa9d9500a46ded5ca	\\?\C:\Program Files\Common Files\microsoft shared\Filters\VISFILT.DLL.PLAY, c:\program files\common files\microsoft shared\filters\visfilt.dll.play	Dropped File	5957.76 KB	application/octet-stream	Access, Create, Write	CLEAN
18cb7162956589ec12aeadd06a027cf157944b7488523cf7b5e83bf48aadf339	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab.PLAY, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onotelr.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6f111d690716247d9ce9b9204806d9e1637d4407d322e390e97072efb955b996	\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.PLAY, c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\office64mui.xml.play	Dropped File	2.91 KB	application/octet-stream	Access, Create, Write	CLEAN
a14d3ab03578ceca7baf8746ebbe3675cdc46062f88a384e9a43c8fa0e5a9175	\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab.PLAY, c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\owow64lr.cab.play	Dropped File	2013.21 KB	application/octet-stream	Access, Create, Write	CLEAN
55daccef353405cea13c5788d5bc04be460796c68d2bccd9f3e6de4168abbc50	\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini.PLAY, c:\program files\common files\microsoft shared\stationery\desktop.ini.play	Dropped File	1.68 KB	application/octet-stream	Access, Create, Write	CLEAN
7e7dc686a11e17b9a331832b2ef499a77a7281821b172f533e8097b3e877d1cd	c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.play, \\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab.PLAY	Dropped File	5635.40 KB	application/octet-stream	Access, Create, Write	CLEAN
b53f10229a068461c30ccd6e2e98d66fd16dd830a2e317d0a1d57d2fe967a105	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY, c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\setup.xml.play	Dropped File	2.65 KB	application/octet-stream	Access, Create, Write	CLEAN
daae6a0b3b114d4217580f289161705f1ad82320a57e4d69a84418dd4b2f7612	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\setup.xml.play, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File	28.18 KB	application/octet-stream	Access, Create, Write	CLEAN
80c1dd82510d1b437178ec1c46333206fcf367e4901638ace4d669e0e5643123	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab.PLAY, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officelr.cab.play	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH02298_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\bs00443_.wmf.play	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA01130_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01772_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\vba\vba7.1\vbeui.dll.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01145_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0107042.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341534.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\arctic\arctic.elm.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\DataModel\Cartridges\sybase.xsl.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0105530.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\pkeyconfig-office.xrm-ms.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\COMPASS\PREVIEW.GIF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01176_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0152590.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0153305.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na01358_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\layers\preview.gif.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\an04225_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na02356_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0187825.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\bl00254_.wmf.play	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02058u.bmp.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\TRANSLAT\MSB1CORE.DLL.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\$recycle.bin\s-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd00255_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0105250.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0099181.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VBA\VBA7.1\1033\VBENDF98.CHM.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0105526.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\RMNSQUE\PREVIEW.GIF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PE06049_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na02451_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0164153.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph03425i.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\compass\thmbnail.png.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02208u.bmp.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\vba\vba7.1\1033\fm20.chm.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\DD01181_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0182902.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0239935.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\bd08773_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0285782.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\DD01585_.WMF.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\cascade\thmbnail.png.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099147.JPG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\AFTRNOON\AFTRNOON.INF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BS00076_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ag00120_.gif.play	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0172193.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0188667.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0152702.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\BL00524_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0099168.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\fd01084_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AG00129_.GIF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\office16\expsrv.dll.play	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\OSMUX.en-us\OSMUXMUI.XML.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\setup.xml.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\NETWORK\NETWORK.INF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\capsules\preview.gif.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0212601.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0105294.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Microsoft Office\Office16\MSOHEV.DLL.PLAY	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0106020.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0239955.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\PROFILE\THMBNAIL.PNG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0199469.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0281243.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.xml.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01265u.bmp.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Microsoft Office\Office16\ONLNTCOMLIB.DLL.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na02426_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0158071.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0199423.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.cab.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0281638.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\RADIAL\PREVIEW.GIF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AN01174_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382966.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na00417_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\na01066_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA02404_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.HLP.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0282932.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0197983.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\pe00686_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\OPTINPS.DLL.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd00256_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\PROOF\MSWDS_ES.LEX.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AG00037_.GIF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0178932.JPG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0196060.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\bd08758_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0187863.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\DataModel\Resources\1033\msmdsrvi_xl.rll.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\accessmuiset.xml.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\pss10r.chm.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.CNT.PLAY	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\BOOTSECT.BAK.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft analysis services\as oledb\110\resources\1033\msmdsrv.rll.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\FLTLDR.EXE.PLAY	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0199307.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0107280.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\HH00669_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\grphflt\ms.gif.play	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\rmnsque\thmbnail.png.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0107526.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\pe02169_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0200467.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0151041.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PARNT_03.MID.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\WATERMAR\WATERMAR.ELM.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0090781.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\NA02373_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02748g.gif.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0198102.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0177257.JPG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\pe00720_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.xml.play	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0179963.JPG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.PLAY	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0101861.bmp.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\capsules\thmbnail.png.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0212953.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0178460.JPG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0217262.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\compass\compass.elm.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0182888.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AN01184_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\office16\office setup controller\office.en-us\setup.chm.play	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0281632.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\WATERMAR\THMBNAIL.PNG.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\dd01166_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\fd02158_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\canyon\thmbnail.png.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\AN01251_.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0152890.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382958.jpg.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\euro\msoeuro.dll.play	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0232393.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\schol_02.mid.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\fd00090_.wmf.play	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
\\?\C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0233512.WMF.PLAY	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

Reduced dataset

Process

Process Name	Commandline	Verdict
006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe	"C:\Users\RDhJ0CNFevzX\Desktop\006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.20 / 2022-08-26 12:47:07
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.21 / 2022-08-29 08:08:35
YARA Built-in Ruleset Version	4.6.1.20

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows