MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe**
ID	#6191366
MD5	a8b3b71860ca65a9e5e56fa3e27cd92b
SHA1	8a5bd8bf26eceaa7adff6e59227646155d220f3e
SHA256	9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3
File Size	164.50 KB
Report Created	2022-11-23 13:40 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 109 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 448 files by appending the extension ".d0nut".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Anti Analysis	Tries to evade debugger	1	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe hides thread via API "NtSetInformationThread".			
3/5	Anti Analysis	Modifies native system functions	1	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies native system functions, possibly to evade hooking.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	2	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe makes a direct system call to "NtMapViewOfSection". • (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe makes a direct system call to "NtOpenSection".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe creates mutex with name "97207d4e-77b3-4a2a-7565-4a7cc790369b".			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\q5JyUTfUVg.gif.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\uKGfqoiC-X.png.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\WooNjQ9N.gif.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\Filters\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ar-SA\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\bg-BG\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\cs-CZ\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ar-SA\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\Alphabet.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\Content.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\FlickAnimation.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\bg-BG\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\hwrcommonlm.dat.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\cs-CZ\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\hwrenclm.dat.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\hwrlatinlm.dat.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\hwrusalm.dat.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\da-DK\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\de-DE\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-GB\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\da-DK\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\hwrusash.dat.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\de-DE\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-GB\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\el-GR\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsar.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\es-ES\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\el-GR\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\boxed-correct.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\es-MX\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\boxed-delete.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipscat.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\es-ES\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipschs.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\boxed-split.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipscht.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\es-MX\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\correct.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\boxed-join.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\delete.avi.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipscsy.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\et-EE\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\fi-FI\d0nut.html".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsdan.xml.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\et-EE\tipresx.dll.mui.d0nut".
- (Process #1) 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe modifies "\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\FlickLearningWizard.exe.mui.d0nut".

Mitre ATT&CK Matrix

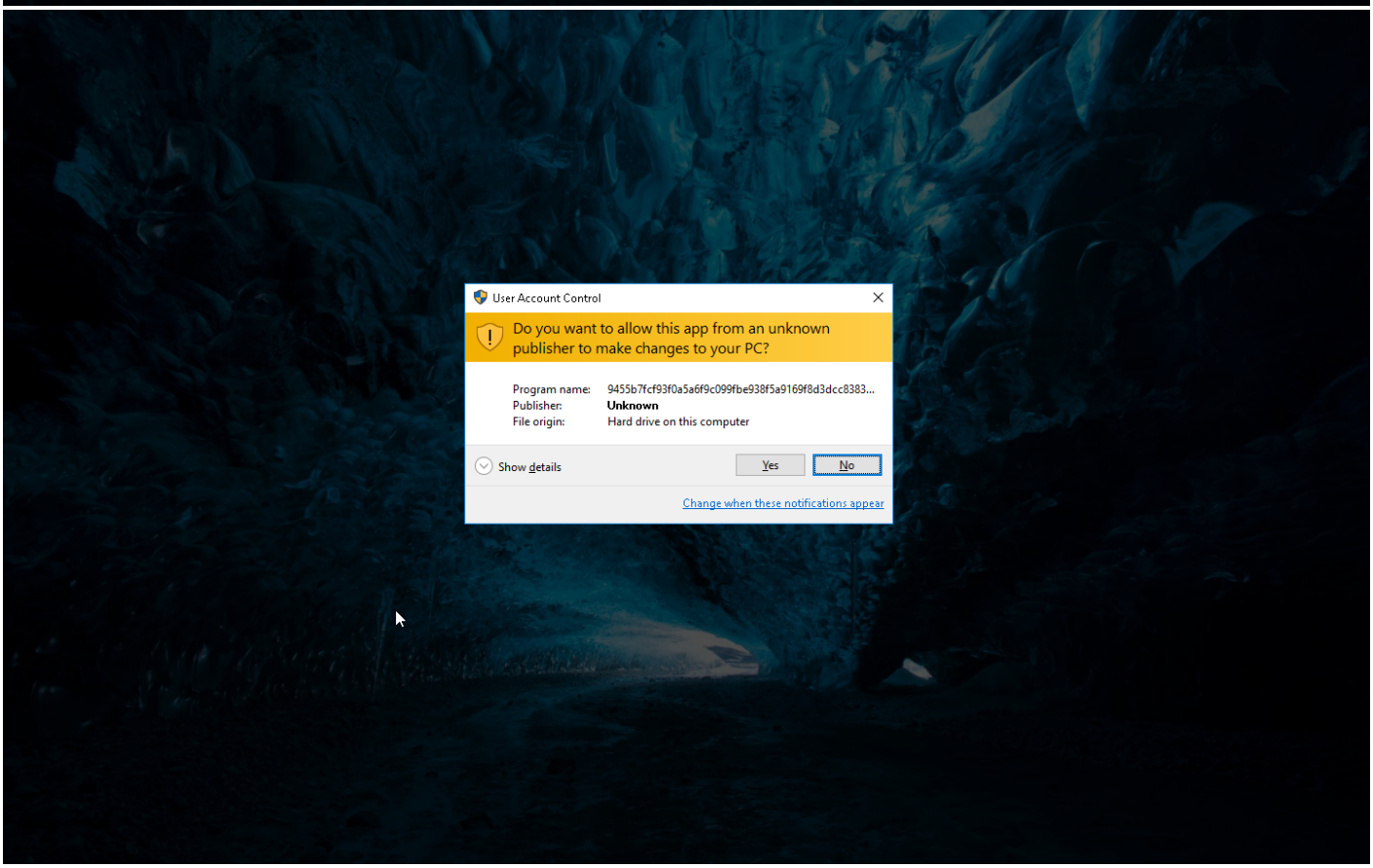
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
											#T1486 Data Encrypted for Impact

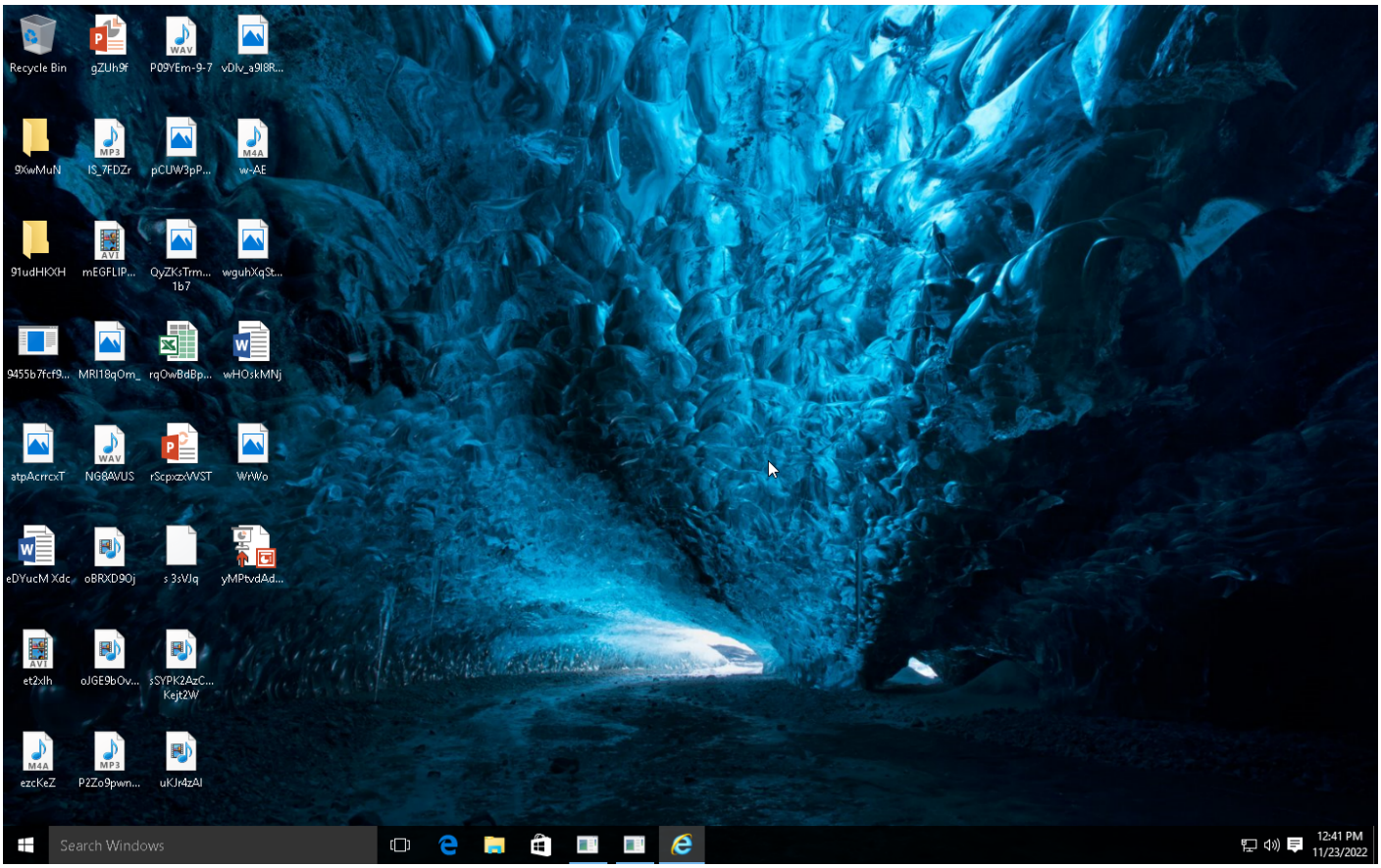
Sample Information

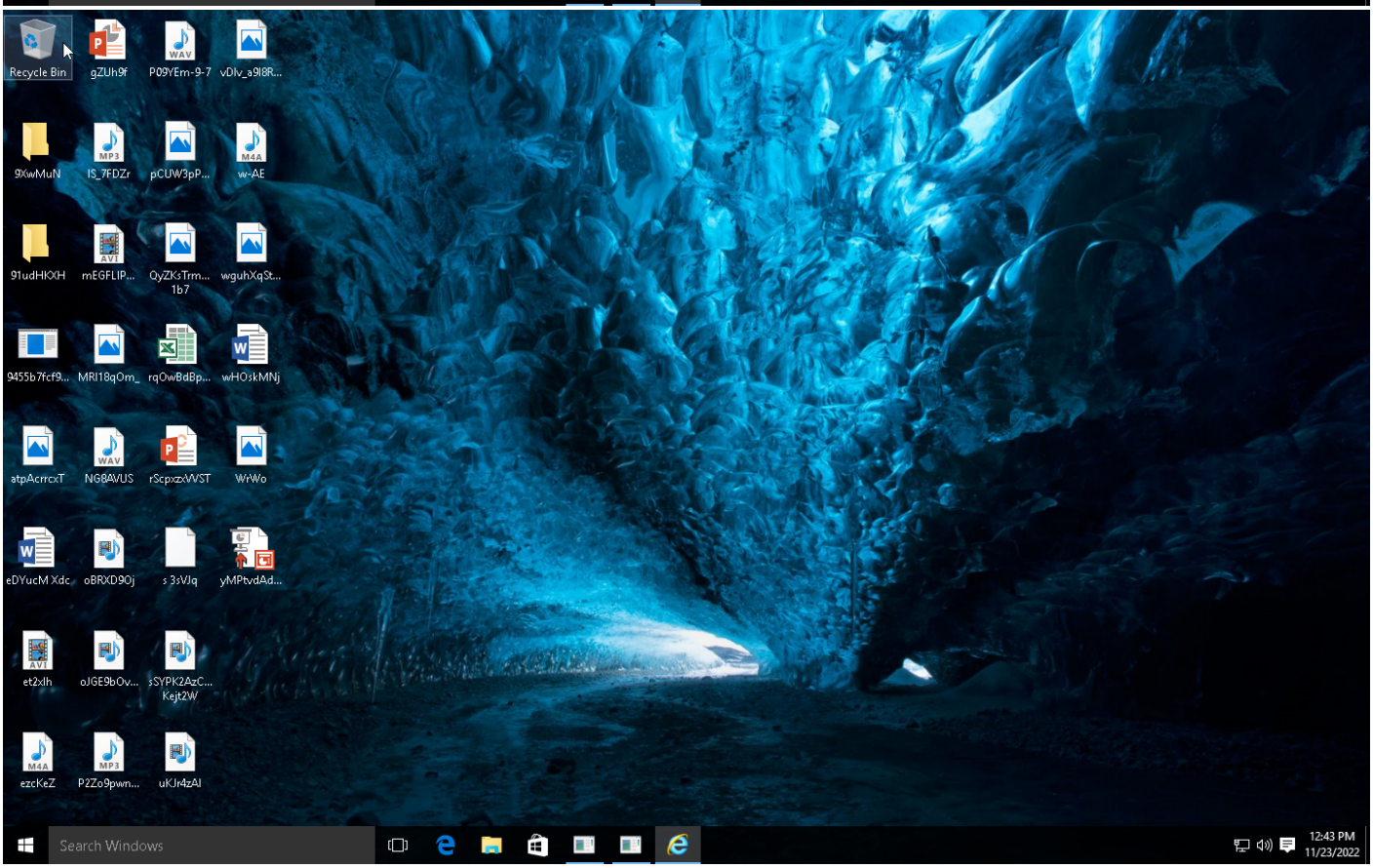
ID	#6191366
MD5	a8b3b71860ca65a9e5e56fa3e27cd92b
SHA1	8a5bd8bf26eceaa7adff6e59227646155d220f3e
SHA256	9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3
SSDeep	1536:mW3XOHHUyrdRpnlsMRgE8Kl70w+ipXEI2W/GxHt/nyaY6uJvtrk3GwzRa0SOO+8W:meXlvxRzMnlQiP29N/yQGwztfO+xV
File Name	9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe
File Size	164.50 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2022-11-23 13:40 (UTC+1)
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: 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc8383...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
gZUh9f
P09YEm-9-7
vDlv_a9l8R...
9XwMuN
IS_7FDZr
pCUW3pP...
w-AE
91udHIXH
mEGFLIP...
QyZKsTrm...
1b7
wguhXqSt...
9455b7fcf9...
MRI18qOm_
rqOwBdBp...
wHOskMNj
atpAcrrcxT
NG8AVUS
rScpxzxWST
WrWo
eDYucM Xdc
oBRXD90j
s 3sVJq
yMPtvdAd...
et2xlh
oJGE9bOv...
sSYPK2AzC...
Kejt2W
ezcKeZ
P2Zo9pwn...
uKJr4zAl
Search Windows
12:41 PM
11/23/2022


Recycle Bin
gZUh9f
P09YEm-9-7
vDlv_a9l8R...
9XwMuN
IS_7FDZr
pCUW3pP...
w-AE
91udHIXH
mEGFLIP...
QyZKsTrm...
1b7
wguhXqSt...
9455b7fcf9...
MRI18qOm_
rqOwBdBp...
wHOskMNj
atpAcrrcxT
NG8AVUS
rScpxzxWST
WrWo
eDYucM Xdc
oBRXD90j
s 3sVJq
yMPtvdAd...
et2xlh
oJGE9bOv...
sSYPK2AzC...
Kejt2W
ezcKeZ
P2Zo9pwn...
uKJr4zAl
Search Windows
12:43 PM
11/23/2022

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

1 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

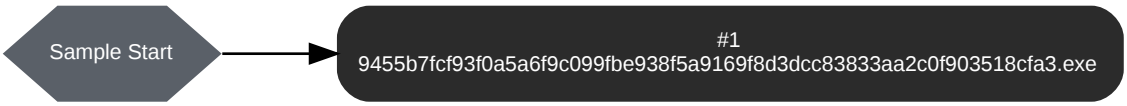
0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://fonts.googleapis.com/css?family=Oswald:300	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72704, Reason: Analysis Target
Unmonitor End Time	End Time: 312850, Reason: Terminated by timeout
Monitor duration	240.15s
Return Code	Unknown
PID	3464
Parent PID	1648
Bitness	64 Bit

Dropped Files (80)

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.d0nut	576.75 KB	87d375b7b346abf41864314526f300b6a1625402ed4878c699d4ee22db5ff686	✖
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.msi.d0nut	1196.07 KB	e5081d8b0eafb6648e0947c96c5026bbea4c274d415c7fdf98c08e5411b0f9af	✖
c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	1.67 KB	2905c1553bcfd45a0bc1a3b4c771b1efde790260ba476850b27d983b4e7d8107	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.msi.d0nut	2060.07 KB	bd4cf764d94c07fc3bab6bf158ffbef5e90cc42a592bc06e06ca35f68843c5ed	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.msi.d0nut	1036.07 KB	987fddc53c054305b5c6e77db77ff9bd2d9d0262e67402c32d80e5728cae2166	✖
c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.xml.d0nut	1.69 KB	c6572e39b5a263e6fe31ebb86913a6322dd62c06f98cfdeef29e4a2a881374f2	✖
c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onotelr.cab.d0nut	10240.00 KB	ab1d9d2952cfdc247b23dd622d28fb6f8c33794ccf6ed54be525841b3276f31c	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.msi.d0nut	2052.07 KB	19094ab9afffb857d0bcd586d38421212d1ee3575d5c61e141c4e2cd76a4833a	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	2.09 KB	e8047fcf0695ce482e519153b4eebf9463d6b63b3df46b152442421f898f51b9	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab.d0nut	5634.41 KB	45875d9ada8af0e247d56f0396fb94991e6b177ce04b0e60a46908bf222035cc	✖
c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	1.82 KB	7338d7c8dbfdbbfed45f2b806aa893af33bec7e7558978253b68e4694bee62d8	✖
c:\bootnxt.d0nut	73 bytes	65f97d3bd1fb31d4ef8ccd34f6aa5a52210adcc5435ac427e6cb91e7811b3f32	✖
c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.xml.d0nut	1.17 KB	a2553db94b2701b1407a432a84318e08c84c0e7c85fe8a37309418c5f8cf3ca9	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.xml.d0nut	4.95 KB	3c3c9ae7e15b17d57a224f80d47a706f1f253e3961b02affa59281f1007d8d5a	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.msi.d0nut	2332.07 KB	27c81b65857d65d9d50f2d028d5ed4ecb1bc77850842e4808f23a9780d44879b	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi.d0nut	2328.07 KB	d04e0ed244c3405f22e1b733ab3c8d9c2de8346920d0769092d2bd24ec07c69e	✖

File Name	File Size	SHA256	YARA Match
c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.msi.d0nut	2332.07 KB	755e508b4c8fb3860fbb2f609e53988b3994a9b0417ed4142430c878d748584d	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.d0nut	1.84 KB	b01f794f185fa7665b78458e4e9586814f521e2447757a3ee401675d585eff08	✖
\\?\C:\Boot\es-MX\d0nut.html	4.21 KB	4557bcc711ce0eb7179a08f91f4a2eb70dde5b2fc41d2d34e9bcd38100301323	✖
c:\boot\bcd.log1.d0nut	72 bytes	f6359c3a49afd956b136c186fe56799a94878e0edd723f6ea6b2fc50f4793eb0	✖
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemui.xml.d0nut	5.22 KB	06d7f8d1def4be31653b2fb2c36259cff2975b20d27495c1c11f9149b452c802	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.msi.d0nut	10240.00 KB	60356c742c70c04257b4f87296e27deeefbd5b08d5b758abbcc8a4fda6c294de	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.d0nut	1.59 KB	ffa9f63865ef7a59d37172f1a8e8e2bdc4cae42c68c9c912bb15a39736e357cb	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	1.82 KB	48ebdcaa84c28915846aab5c855e9a8e82945112d2dd6606b1380f62fce4e8e5	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\owow64ww.cab.d0nut	10240.00 KB	8c537555f07216f4879ec37e413c807d449af8038adc340ff5fa6b66553d47f3	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.cab.d0nut	10240.00 KB	59767db062af296225d5e6d66b7422b6a53a37711656b39f6fddf2d6854c0bdd	✖
c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	2.06 KB	c64fb050f21557db292f11c468e3851518100b8ee27150cf0b424ba9a47c0faa	✖
c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\office64mui.msi.d0nut	1196.07 KB	193115e20331c8f2326fb1060753f1db2568a86482fd653a14285a7c0c637a63	✖
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officelr.cab.d0nut	8364.30 KB	b890c24a447af94360168ee8038ad78c59d27fb88520644356f15d443664b836	✖
\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.d0nut	3915.29 KB	d502b44d3b84b37bd78683ccb06a58c4022e6a3505faf8036dae3da66a12c2c9	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.msi.d0nut	2348.07 KB	c7a138da13be4c58eb5351a52473a70e415c0a3f799f904b60195760d6269860	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	6.00 KB	9f0043f1179ff918d6b3920680a2d34a5f5629ed141191436374fcf9a4c6ce09	✖
c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.cab.d0nut	16.49 KB	f4274bb8a5d0f8d2fe5191a893eabeb88a7907fe16289799851338710a9efbe9	✖
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.d0nut	9843.56 KB	f53276acbbc86c06733eccd958bc86a14801b34383d5413609c174a7729abe0f	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.cab.d0nut	10240.00 KB	cb8a0e2145e22387f4e28649c06bef324de3089335c4ffb2d5f402e7caed0097	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.xml.d0nut	1.07 KB	04e0351658716ae2b598d28274abfdd0abf02675851c67c993b84a0c4ec89297	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	3.85 KB	b7cf3eedc5b42573dda214557bb8d72bf12f7a4a039d48a5d02834002e0989f5	✖
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	2.19 KB	c115e46bbf9a2635078b6b2369ca02430146eec032c11e67a74d29369f4da22c	✖
\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.d0nut	6162.30 KB	160388f72da6c52f2a3fca26842194bad91f55c04fe25edd9124cfd53cef713d	✖
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	1.84 KB	beaf788081c34c51d4aa3e8964871edc46b140d07819adeb2fb91db6f581b644	✖
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.d0nut	3852.07 KB	355c16c71a09034d2ac8af154239bb9f680c22f58fdcf3e7e9f9c7bb147d19f3	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	2.49 KB	32d34cc529489341c43d487ffe37594237f859627d3f49734fd204ab82f42c35	✖
c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\infopathmui.xml.d0nut	1.27 KB	9dbe90195b2401f21b5dcb446619b97c80860e1e56f89454510a936a392b784b	✖
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.xml.d0nut	1.26 KB	ccb4eff94a57e7b8d509feb75d7f72612c5f9dfed12feb17a878b86b0dce8485	✖
\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.d0nut	1.49 KB	d839f678e7fb7461609cc9726ae1edefa9f80a31d47f27a3b428431536d7b47f	✖
c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.msi.d0nut	2324.07 KB	ef9d4d149bb6880d98ba13076db5f61a0a92578d2d61a6f8b9a984319a97dfec	✖
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.cab.d0nut	10240.00 KB	17338ad3d6eac03f98152032cc512aca0fb7f708bba4a77f57ff2f4d3ce3261c	✖
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.d0nut	852.57 KB	f777c764fc09ae18dd259955537abdae5e7b7ace8252143aa4d6ac0aaf7b4f9a	✖
\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	2.78 KB	9f4d8d5b33744412f9fc82a6cea5dd023efc39a4edcc5189358e079c457fdfae	✖
c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.msi.d0nut	2328.07 KB	0cd30e3d92aacd04dae8b3499b1d70c751b1d790f515e95f46fbc336fcf7251d	✖
\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.d0nut	3820.04 KB	f74352e50a2296003e61d984df325db56fa47adb6cfdaef604e32bf8134490ea	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.msi.d0nut	2060.07 KB	1064d56b7138424886fa0b26370275f9eef49a3ab4ce7ec3d59afd2ffa3ac69c	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\setup.xml.d0nut	27.20 KB	54977a5d08ddbf40eeba22a525dc3a797b78410cfe6c62a36adfdb2cdf914052	✖
c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.xml.d0nut	1.69 KB	fcb9b9f619546bdec030ffb7ca8f55d2ad58dd985f2db0b45264e097b8df4149	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.d0nut	2764.07 KB	2764333de35b33a89532860774d2c9ccb7b74d3f5db14556553807c30ec068be	✖
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.xml.d0nut	1.70 KB	b20a8d2ab16c18794555a7d72d76053f0b990514a157e96c08fbae6228363dc3	✖
\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.d0nut	626.62 KB	b8a3a7a4530c6f46bd2390a6b848078a2dd72265f625a38a8c3cf3acaf22786e	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.d0nut	3478.24 KB	f6def35acdbf186ed62112d70d7740af436f4886e2219299af4c69445973f5f9	✖
\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi.d0nut	2352.07 KB	5efac0fc21da99dfb67369cfb6c66e7b614d62f0f0cbeaef09c6ddbbaa88c946	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.d0nut	1.81 KB	ffa9495562fcfcbc6d43e5674fcd52db143813bd21b669ea61886fa7ccf60df4	✖
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi.d0nut	2332.07 KB	613964fc73dc57f6547cc090f02f7bf47ac6b9d7e378ea63583481d5d34d9467	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww2.cab.d0nut	10240.00 KB	f47a7aedc80a18e945d9c12c90918e6c74cdf444afeac3a9841a7ac933258eb2	✖
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.xml.d0nut	2.84 KB	fd2d11ff1daa7bfca82a5e979cb2f4e067ea831833f0e826851f99391f39f509	✖
\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.d0nut	1.17 KB	dc97053101db65f0f6d5a8be42c7b18974c3f9de0dd66f93783c86a1daee3567	✖
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.xml.d0nut	16.78 KB	89a84d5ebbde029a5faacfab06d61e4ed26038f5176cfa70a72116d680577ac0	✖
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.d0nut	328.50 KB	0902b0e2f800e0f8dfb728d0b1f28e717b5784479e050a3f8a726881d1c28501	✖

File Name	File Size	SHA256	YARA Match
\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.d0nut	2.13 KB	f65a652aa2f29cb790b5dd5f2f6e563e13cc992b15c9c7e8c71cae45a96a380b	✖
c:\program files\java\jre1.8.0_171\lib\images\cursors\cursors.properties.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\ext\cldrdata.jar.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkNoDrop32x32.gif.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\jfr\profile.jfc.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\java\jre1.8.0_171\lib\jfr\default.jfc.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\ext\jaccess.jar.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\java\jre1.8.0_171\lib\images\cursors\invalid32x32.gif.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\security\blacklist.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\java\jre1.8.0_171\lib\images\cursors\win32_linkdrop32x32.gif.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
\\?\C:\Program Files\Java\jre1.8.0_171\lib\ext\jfxrt.jar.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\java\jre1.8.0_171\lib\images\cursors\win32_copydrop32x32.gif.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\common files\microsoft shared\office16\cultures\office.odf.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\program files\common files\services\verisign.bmp.d0nut	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
File	3092
Module	3
System	3
-	41
-	881
Mutex	2
-	280

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3	C:\Users\RDhJ0CNFevzX\Desktop\9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe	Sample File	164.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
87d375b7b346abf41864314526f300b6a1625402ed4878c699d4ee22db5ff686	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\pkeyconfig-office.xrm-ms.d0nut, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\pkeyconfig-office.xrm-ms.d0nut	Dropped File	576.75 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e5081d8b0eafb6648e0947c96c5026bbea4c274d415c7fdf98c08e5411b0f9af	\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\OSMMUI.msi.d0nut, c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.msi.d0nut	Dropped File	1196.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
2905c1553bcfd45a0bc1a3b4c771b1efde790260ba476850b27d983b4e7d8107	c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\setup.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000FF1CE}-C\Setup.xml.d0nut	Dropped File	1.67 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
bd4cf764d94c07fc3bab6bf158ffbef5e90cc42a592bc06e06ca35f68843c5ed	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.fr\Proof.msi.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.msi.d0nut	Dropped File	2060.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
987fddc53c054305b5c6e77db77ff9bd2d9d0262e67402c32d80e5728cae2166	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proofing.msi.d0nut	Dropped File	1036.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c6572e39b5a263e6fe31ebb86913a6322dd62c06f98cfdeef29e4a2a881374f2	c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.xml.d0nut	Dropped File	1.69 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ab1d9d2952cfdc247b23dd622d28fb6f8c33794ccf6ed54be525841b3276f31c	c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onotelr.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000FF1CE}-C\OnoteLR.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
19094ab9afffb857d0bcd586d38421212d1ee3575d5c61e141c4e2cd76a4833a	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.en\Proof.msi.d0nut	Dropped File	2052.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
e8047fcf0695ce482e519153b4eebf9463d6b63b3df46b152442421f898f51b9	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Dropped File	2.09 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
45875d9ada8af0e247d56f0396fb94991e6b177ce04b0e60a46908bf222035cc	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelLR.cab.d0nut, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excellr.cab.d0nut	Dropped File	5634.41 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
7338d7c8dbfdbbfed45f2b806aa893af33bec7e7558978253b68e4694bee62d8	c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\setup.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-000000FF1CE}-C\Setup.xml.d0nut	Dropped File	1.82 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
65f97d3bd1fb31d4ef8ccd34f6aa5a52210adcc5435ac427e6cb91e7811b3f32	c:\bootnxt.d0nut, \\?\C:\BOOTNXT.d0nut	Dropped File	73 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
a2553db94b2701b1407a432a84318e08c84c0e7c85fe8a37309418c5f8cf3ca9	c:\msocache\all users\{90160000-00e1-0409-0000-0000000ff1ce}-c\osmmui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000000FF1CE}-C\OSMMUI.xml.d0nut	Dropped File	1.17 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
3c3c9ae7e15b17d57a224f80d47a706f1f253e3961b02affa59281f1007d8d5a	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\Office64WW.xml.d0nut	Dropped File	4.95 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
27c81b65857d65d9d50f2d028d5ed4ecb1bc77850842e4808f23a9780d44879b	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000000FF1CE}-C\OneNoteMUI.msi.d0nut, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onenotemui.msi.d0nut	Dropped File	2332.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d04e0ed244c3405f22e1b733ab3c8d9c2de8346920d0769092d2bd24ec07c69e	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-000000000FF1CE}-C\InfoPathMUI.msi.d0nut, c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\infopathmui.msi.d0nut	Dropped File	2328.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
755e508b4c8fb3860fbb2f609e53988b3994a9b0417ed4142430c878d748584d	c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-000000000FF1CE}-C\PowerPointMUI.msi.d0nut	Dropped File	2332.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b01f794f185fa7665b78458e4e9586814f521e2447757a3ee401675d585eff08	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000000FF1CE}-C\OneNoteMUI.xml.d0nut, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onenotemui.xml.d0nut	Dropped File	1.84 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
4557bcc711ce0eb7179a08f91f4a2eb70dde5b2fc41d2d34e9bcd38100301323	\\?\C:\Boot\es-MX\d0nut.html, \\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-000000000FF1CE}-C\d0nut.html, \\?\C:\Boot\nb-NO\d0n... ...oof.es\d0nut.html, \\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-000000000FF1CE}-C\Access.en-us\d0nut.html, c:\users\d0nut.html	Dropped File	4.21 KB	text/html	Access, Create, Write	CLEAN
f6359c3a49afd956b136c186fe56799a94878e0edd723f6ea6b2fc50f4793eb0	c:\boot\bcd.log1.d0nut, \\?\C:\Boot\BCD.LOG1.d0nut, \\?\C:\Boot\BCD.LOG2.d0nut, c:\boot\bcd.log2.d0nut	Dropped File	72 bytes	application/octet-stream	Access, Create, Read, Write	CLEAN
06d7f8d1def4be31653b2fb2c36259cff2975b20d27495c1c11f9149b452c802	c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000000FF1CE}-C\OfficeMUI.xml.d0nut	Dropped File	5.22 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
60356c742c70c04257b4f87296e27deeefbd5b08d5b758abbcc8a4fda6c294de	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\ProPlusWW.msi.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ffa9f63865ef7a59d37172f1a8e8e2bdc4cae42c68c9c912bb15a39736e357cb	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000000FF1CE}-C\Proof.en\Proof.xml.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.xml.d0nut	Dropped File	1.59 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
48ebdcaa84c28915846aab5c855e9a8e82945112d2dd6606b1380f62fce4e8e5	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-0019-0409-0000-0000ff1ce}-c\setup.xml.d0nut	Dropped File	1.82 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
8c537555f07216f4879ec37e413c807d449af8038adc340ff5fa6b66553d47f3	c:\msocache\all users\{90160000-0011-0000-0000-0000ff1ce}-c\owow64ww.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\OWOW64WW.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
59767db062af296225d5e6d66b7422b6a53a37711656b39f6fddf2d6854c0bdd	c:\msocache\all users\{90160000-002c-0409-0000-0000ff1ce}-c\proof.es\proof.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.es\Proof.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c64fb050f21557db292f11c468e3851518100b8ee27150cf0b424ba9a47c0faa	c:\msocache\all users\{90160000-00e1-0409-0000-0000ff1ce}-c\setup.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\Setup.xml.d0nut	Dropped File	2.06 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
193115e20331c8f2326fb1060753f1db2568a86482fd653a14285a7c0c637a63	c:\msocache\all users\{90160000-0116-0409-1000-0000ff1ce}-c\office64mui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-000000FF1CE}-C\Office64MUI.msi.d0nut	Dropped File	1196.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b890c24a447af94360168ee8038ad78c59d27fb88520644356f15d443664b836	c:\msocache\all users\{90160000-0115-0409-0000-0000ff1ce}-c\officelr.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\OfficeLR.cab.d0nut	Dropped File	8364.30 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d502b44d3b84b37bd78683ccb06a58c4022e6a3505faf8036dae3da66a12c2c9	\\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlkLR.cab.d0nut, c:\msocache\all users\{90160000-001a-0409-0000-0000ff1ce}-c\outlklr.cab.d0nut	Dropped File	3915.29 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c7a138da13be4c58eb5351a52473a70e415c0a3f799f904b60195760d6269860	c:\msocache\all users\{90160000-001b-0409-0000-0000ff1ce}-c\wordmui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\WordMUI.msi.d0nut	Dropped File	2348.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9f0043f1179ff918d6b3920680a2d34a5f5629ed1411914363 74fcf9a4c6ce09	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000ff1ce}-c\setup.xml.d0nut	Dropped File	6.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f4274bb8a5d0f8d2fe5191a893eabeb88a7907fe16289799851338710a9efbe9	c:\msocache\all users\{90160000-00e1-0409-0000-0000ff1ce}-c\osmmui.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-000000FF1CE}-C\OSMMUI.cab.d0nut	Dropped File	16.49 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f53276acbbc86c06733eccd958bc86a14801b34383d5413609c174a7729abe0f	c:\msocache\all users\{90160000-001b-0409-0000-0000ff1ce}-c\wordlr.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\WordLR.cab.d0nut	Dropped File	9843.56 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
cb8a0e2145e22387f4e28649c06bef324de3089335c4ffb2d5f402e7caed0097	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.en\Proof.cab.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000ff1ce}-c\proof.en\proof.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
04e0351658716ae2b598d28274abfdd0abf02675851c67c993b84a0c4ec89297	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proofing.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proofing.xml.d0nut	Dropped File	1.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b7cf3eedc5b42573dda214557bb8d72bf12f7a4a039d48a5d02834002e0989f5	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\setup.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\Setup.xml.d0nut	Dropped File	3.85 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
c115e46bbf9a2635078b6b2369ca02430146eec032c11e67a74d29369f4da22c	\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Dropped File	2.19 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
160388f72da6c52f2a3fca26842194bad91f55c04fe25edd9124cfd53cef713d	\\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PptLR.cab.d0nut, c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\pptlr.cab.d0nut	Dropped File	6162.30 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
beaf788081c34c51d4aa3e8964871edc46b140d07819adeb2fb91db6f581b644	\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Dropped File	1.84 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
355c16c71a09034d2ac8af154239bb9f680c22f58fdcf3e7e9f9c7bb147d19f3	\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Office64WW.msi.d0nut, c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\office64ww.msi.d0nut	Dropped File	3852.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
32d34cc529489341c43d487ffe37594237f859627d3f49734fd204ab82f42c35	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Dropped File	2.49 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9dbe90195b2401f21b5dcb446619b97c80860e1e56f89454510a936a392b784b	c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\infopathmui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-000000FF1CE}-C\InfoPathMUI.xml.d0nut	Dropped File	1.27 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ccb4eff94a57e7b8d509feb75d7f72612c5f9dfed12feb17a878b86b0dce8485	c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-000000FF1CE}-C\DCFMUI.xml.d0nut	Dropped File	1.26 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
d839f678e7fb7461609cc9726ae1edefa9f80a31d47f27a3b428431536d7b47f	\\?\C:\MSOCache\All Users\{90160000-00E2-0409-0000-000000FF1CE}-C\OSMUXMUI.xml.d0nut, c:\msocache\all users\{90160000-00e2-0409-0000-0000000ff1ce}-c\osmuxmui.xml.d0nut	Dropped File	1.49 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
ef9d4d149bb6880d98ba13076db5f61a0a92578d2d61a6f8b9a984319a97dfec	c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000FF1CE}-C\GrooveMUI.msi.d0nut	Dropped File	2324.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
17338ad3d6eac03f98152032cc512aca0fb7f708bba4a77f57ff2f4d3ce3261c	c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.fr\Proof.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f777c764fc09ae18dd259955537abdae5e7b7ace8252143aa4d6ac0aaf7b4f9a	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000FF1CE}-C\GrooveLR.cab.d0nut, c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovelr.cab.d0nut	Dropped File	852.57 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
9f4d8d5b33744412f9fc82a6cea5dd023efc39a4edcc5189358e079c457fdfae	\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\Setup.xml.d0nut, c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Dropped File	2.78 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0cd30e3d92aacd04dae8b3499b1d70c751b1d790f515e95f46fbc336fcf7251d	c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-000000FF1CE}-C\DCFMUI.msi.d0nut	Dropped File	2328.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f74352e50a2296003e61d984df325db56fa47adb6cfdaef604e32bf8134490ea	\\?\C:\MSOCache\All Users\{90160000-0044-0409-0000-000000FF1CE}-C\InfLR.cab.d0nut, c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\inflr.cab.d0nut	Dropped File	3820.04 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
1064d56b7138424886fa0b26370275f9eef49a3ab4ce7ec3d59afd2ffa3ac69c	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.es\Proof.msi.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.msi.d0nut	Dropped File	2060.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
54977a5d08ddbf40eeba22a525dc3a797b78410cfe6c62a36adfdb2cdf914052	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\setup.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Setup.xml.d0nut	Dropped File	27.20 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
fcb9b9f619546bdec030ffb7ca8f55d2ad58dd985f2db0b45264e097b8df4149	c:\msocache\all users\{90160000-0018-0409-0000-0000000ff1ce}-c\powerpointmui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PowerPointMUI.xml.d0nut	Dropped File	1.69 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
2764333de35b33a895328606774d2c9ccb7b74d3f5db14556553807c30ec068be	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.d0nut, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlookMUI.msi.d0nut	Dropped File	2764.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b20a8d2ab16c18794555a7d72d76053f0b990514a157e96c08fbae6228363dc3	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.es\Proof.xml.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.es\proof.xml.d0nut	Dropped File	1.70 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
b8a3a7a4530c6f46bd2390a6b848078a2dd72265f625a38a8c3cf3acaf22786e	\\?\C:\MSOCache\All Users\{90160000-0090-0409-0000-000000FF1CE}-C\DCFMUI.cab.d0nut, c:\msocache\all users\{90160000-0090-0409-0000-0000000ff1ce}-c\dcfmui.cab.d0nut	Dropped File	626.62 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f6def35acdbf186ed62112d70d7740af436f4886e2219299af4c69445973f5f9	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PubLR.cab.d0nut, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publr.cab.d0nut	Dropped File	3478.24 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
5efac0fc21da99dfb67369cfb6c66e7b614d62f0f0cbeaef09c6ddbbaa88c946	\\?\C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.msi.d0nut, c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.msi.d0nut	Dropped File	2352.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ffa9495562fcfcbc6d43e5674fcd52db143813bd21b669ea61886fa7ccf60df4	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelMUI.xml.d0nut, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excelmui.xml.d0nut	Dropped File	1.81 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
613964fc73dc57f6547cc090f02f7bf47ac6b9d7e378ea63583481d5d34d9467	\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelMUI.msi.d0nut, c:\msocache\all users\{90160000-0016-0409-0000-0000000ff1ce}-c\excelmui.msi.d0nut	Dropped File	2332.07 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f47a7aedc80a18e945d9c12c90918e6c74cdf444afeac3a9841a7ac933258eb2	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww2.cab.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\ProPsWW2.cab.d0nut	Dropped File	10240.00 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
fd2d11ff1daa7bfca82a5e979cb2f4e067ea831833f0e826851f99391f39f509	c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-001A-0409-0000-000000000FF1CE}-C\OutlookMUI.xml.d0nut	Dropped File	2.84 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
dc97053101db65f0f6d5a8be42c7b18974c3f9de0dd66f93783c86a1daee3567	\\?\C:\MSOCache\All Users\{90160000-00BA-0409-0000-000000FF1CE}-C\GrooveMUI.xml.d0nut, c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.xml.d0nut	Dropped File	1.17 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
89a84d5ebbde029a5faacfab06d61e4ed26038f5176cfa70a72116d680577ac0	c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\proplusww.xml.d0nut, \\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-000000000FF1CE}-C\ProPlusWW.xml.d0nut	Dropped File	16.78 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
688ff2286629fa7e73f11b1795b3f43ae9c9e83b308d4521655610f2b84da6b5	\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-000000FF1CE}-C\Proof.fr\Proof.xml.d0nut, c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.fr\proof.xml.d0nut	Modified File	1.70 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
0902b0e2f800e0f8dfb728d0b1f28e717b5784479e050a3f8a726881d1c28501	\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-000000FF1CE}-C\branding.xml.d0nut, c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\branding.xml.d0nut	Dropped File	328.50 KB	application/octet-stream	Access, Create, Read, Write	CLEAN
f65a652aa2f29cb790b5dd5f2f6e563e13cc992b15c9c7e8c71cae45a96a380b	\\?\C:\MSOCache\All Users\{90160000-001B-0409-0000-000000FF1CE}-C\WordMUI.xml.d0nut, c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.xml.d0nut	Dropped File	2.13 KB	application/octet-stream	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\microsoft shared\ink\fsdefinitions\auxpad.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskclearui.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\currency.data.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\es-ES\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\fr-FR\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\images\cursors\cursors.properties.d0nut	Accessed File, Dropped File, Modified File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\fsdefinitions\osknav.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\microsoft shared\Stationery\OrangeCircles.jpg.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\Fonts\segmono_boot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\ru-ru\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\cmm\GRAY.pf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\graph.emf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\fonts\lucidabrightdemibold.ttf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\charsets.jar.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\peacock.htm.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.msi.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\es-ES\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsrom.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-001a-0409-0000-0000000ff1ce}-c\outlookmui.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\classlist.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\zh-tw\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\Welcome.html.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsptb.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\fonts\lucidabrightregular.ttf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordmui.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\accessmuiset.msi.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsnor.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\fr-ca\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsid.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\fr-FR\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe	Sample File	-	MALICIOUS
\\?\C:\Boot\zh-HK\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\system\ado\adovbs.inc.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\ext\cldrdata.jar.d0nut	Accessed File, Dropped File, Modified File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsrus.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\tr-TR\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\qps-ploc\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\owow64ww.cab.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-00a1-0409-0000-0000000ff1ce}-c\onotelr.cab.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipstr.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\zh-cn\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsfra.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\system\ado\msadox28.tlb.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsjpn.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\ja-JP\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipshrv.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\system\ole db\sqloledb.rll.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\System\msadc\en-US\msdaremr.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\uk-ua\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\th-TH\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\en-US\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\fonts\LucidaBrightItalic.ttf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkNoDrop32x32.gif.d0nut	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\LICENSE.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\sl-SI\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\lv-lv\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\Fonts\cht_boot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipsdeu.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\infopathmui.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\FlickLearningWizard.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\month_calendar.emf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.en\Proof.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\amd64\jvm.cfg.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0044-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\roses.jpg.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\tabtip.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\main\ko-kr.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\it-it\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\join.avi.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\en-US\tabskb.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\insert\insertbase.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\es-ES\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-001b-0409-0000-0000000ff1ce}-c\wordlr.cab.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\Fonts\chs_boot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\de-de\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\vsto\vstoee100.tlb.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\System\msadc\en-US\msaddsr.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ru-RU\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\ipscsy.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\system\ado\msador28.tlb.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\Fonts\segoe_slboot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsel.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\bin\server\classes.jsa.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\flickanimation.avi.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\zh-cn\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\jfr\profile.jfc.d0nut	Accessed File, Dropped File, Modified File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Boot\Fonts\malgunn_boot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\fonts\LucidaBrightDemiItalic.ttf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemui.msi.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0115-0409-0000-0000000ff1ce}-c\officemuiset.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\boot\nl-nl\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-002c-0409-0000-0000000ff1ce}-c\proof.en\proof.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\qps-ploc\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\cmm\linear_rgb.pf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Boot\it-IT\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\flavormap.properties.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0116-0409-1000-0000000ff1ce}-c\office64mui.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0019-0409-0000-0000000ff1ce}-c\publishermui.xml.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\fsdefinitions\auxpad\auxbase.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Stars.htm.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-0011-0000-0000-0000000ff1ce}-c\propsww2.cab.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\oskpredbase.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\hu-hu\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\jfr\default.jfc.d0nut	Accessed File, Dropped File, Modified File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\Stationery\White_Chocolate.jpg.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\lib\fonts\lucidasansdemibold.ttf.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\program files\common files\system\msadc\en-us\msadcor.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS
c:\msocache\all users\{90160000-0117-0409-0000-0000000ff1ce}-c\access.en-us\accessmui.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\release.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\et-EE\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\seyes.emf.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\tr-tr\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\nb-NO\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-00ba-0409-0000-0000000ff1ce}-c\groovemui.msi.d0nut	Accessed File, Dropped File	Access, Create, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
\\?\C:\Program Files\Common Files\microsoft shared\ink\fsdefinitions\main\zh-dayi.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\BCD.LOG.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipscat.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\java\jre1.8.0_171\copyright.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\system\ole db\oledbjvs.inc.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ko-KR\tipresx.dll.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\msocache\all users\{90160000-012b-0409-0000-0000000ff1ce}-c\setup.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.xml.d0nut	Accessed File, Modified File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\branding.xml.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\Program Files\Java\jre1.8.0_171\lib\content-types.properties.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
\\?\C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccLR.cab.d0nut	Accessed File	Access, Create, Read, Write	MALICIOUS
c:\boot\pt-pt\memtest.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\microsoft shared\ink\ipsen.xml.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Boot\en-GB\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\ja-jp\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Common Files\System\ado\msado27.tlb.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\program files\common files\microsoft shared\stationery\wrinkled_paper.gif.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\lt-lt\bootmgr.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
\\?\C:\Program Files\Internet Explorer\en-US\iexplore.exe.mui.d0nut	Accessed File	Access, Create, Write	MALICIOUS
c:\boot\fonts\wgl4_boot.ttf.d0nut	Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://fonts.googleapis.com/css?family=Oswald:300	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
fonts.googleapis.com	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
97207d4e-77b3-4a2a-7565-4a7cc790369b	access	9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe	CLEAN

Process

Process Name	Commandline	Verdict
9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9455b7fcf93f0a5a6f9c099fbe938f5a9169f8d3dcc83833aa2c0f903518cfa3.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	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.1.7 / 2022-10-27 16:01:27
Link Detonation Heuristics Version	4.7.1.8 / 2022-10-30 09:01:20
Smart Memory Dumping Rules Version	4.7.1.7 / 2022-10-27 16:01:27
Config Extractors Version	4.7.1.11 / 2022-11-11 16:05:21
Signature Trust Store Version	4.7.1.8 / 2022-10-30 09:01:20
VMRay Threat Identifiers Version	4.7.1.12 / 2022-11-15 10:04:31
YARA Built-in Ruleset Version	4.7.1.10

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	8.0.1710.11

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