MALICIOUS

Classifications: Ransomware

Threat Names: RagnarLocker

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Ragnar_11_02_2020_40KB.exe**
ID	#3193064
MD5	6171000983cf3896d167e0d8aa9b94ba
SHA1	b155264bbfbad7226b5eb3be2ab38c3ecd9f3e18
SHA256	9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376
File Size	39.50 KB
Report Created	2021-12-27 19:21 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 212 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) ragnar_11_02_2020_40kb.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) ragnar_11_02_2020_40kb.exe renames multiple user files.			
5/5	YARA	Malicious content matched by YARA rules	100	Ransomware

- Rule "RagnarLocker" from ruleset "Ransomware" has matched on the sample itself.
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Boot\BOOTSTAT.DAT".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\g8zbEIxadWk.bmp".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\mFNPUwcV_x85.gif".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Common Files\rgH4x0V6Uom.png".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml".
- Rule "RagnarLockerEncryptedFile" from ruleset "Ransomware" has matched on the modified file "\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml".

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 7168 files by appending the extension ".ragnar_eedcf512".			
5/5	User Data Modification	Modifies Windows automatic backups	1	-
	• (Process #1) ragnar_11_02_2020_40kb.exe deletes Windows volume shadow copies.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Defense Evasion	Accesses physical drive	1	-
	• (Process #1) ragnar_11_02_2020_40kb.exe accesses physical drive "\device\harddisk0\dr0".			
2/5	Defense Evasion	Sends control codes to connected devices	1	-
	• (Process #1) ragnar_11_02_2020_40kb.exe controls device "\\.\PHYSICALDRIVE0" through API DeviceIOControl.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #2) wmic.exe executes WMI query: SELECT * FROM Win32_ShadowCopy.			
1/5	Discovery	Reads system data	1	-
	• (Process #1) ragnar_11_02_2020_40kb.exe reads the cryptographic machine GUID from registry.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) ragnar_11_02_2020_40kb.exe starts (process #2) wmic.exe with a hidden window. • (Process #1) ragnar_11_02_2020_40kb.exe starts (process #3) vssadmin.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #2) wmic.exe enables process privilege "".			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\ar-sa\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\ar-sa\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\bg-bg\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\bg-bg\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\cs-cz\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\cs-cz\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\da-dk\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\da-dk\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\de-de\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\de-de\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\el-gr\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\el-gr\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-gb\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-gb\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\boxed-correct.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\boxed-delete.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\boxed-join.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\boxed-split.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\correct.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\delete.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\flicklearningwizard.exe.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\inkobj.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\inputpersonalization.exe.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\ipseventlogmsg.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\ipsmigrationplugin.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\join.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\micaut.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\mip.exe.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\mshwlatin.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\rtscom.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\shapecollector.exe.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\split.avi.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\tabskb.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\tabtip.exe.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\tipres.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\tiptsf.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\es-es\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\es-es\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\es-mx\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\es-mx\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\et-ee\rgnr_eedcf512.txt".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\et-ee\tipresx.dll.mui.ragnar_eedcf512".
- (Process #1) ragnar_11_02_2020_40kb.exe modifies "c:\program files\common files\microsoft shared\ink\fi-fi\rgnr_eedcf512.txt".

Mitre ATT&CK Matrix

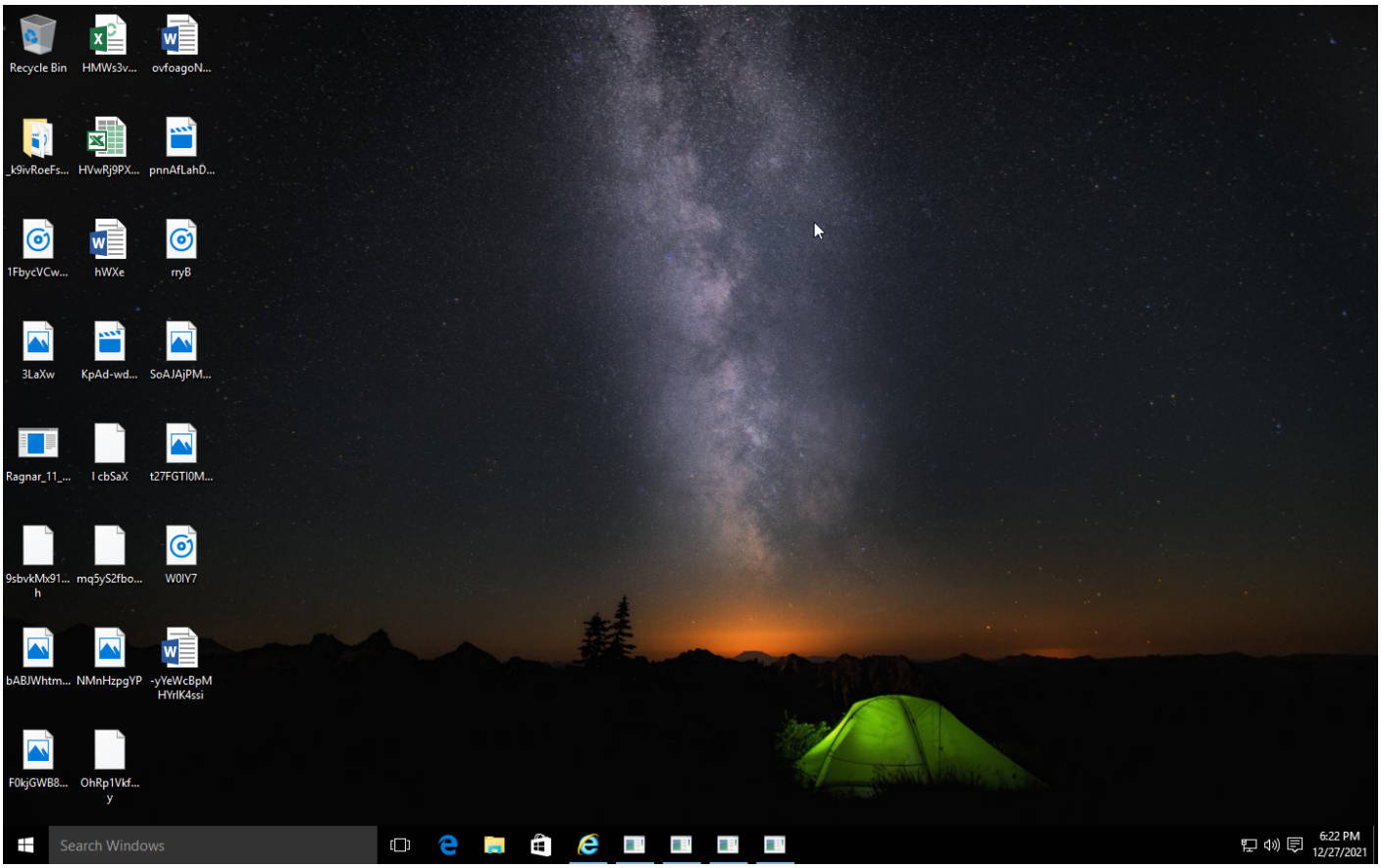
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1006 File System Logical Offsets		#T1082 System Information Discovery					#T1486 Data Encrypted for Impact
				#T1143 Hidden Window		#T1012 Query Registry					#T1490 Inhibit System Recovery

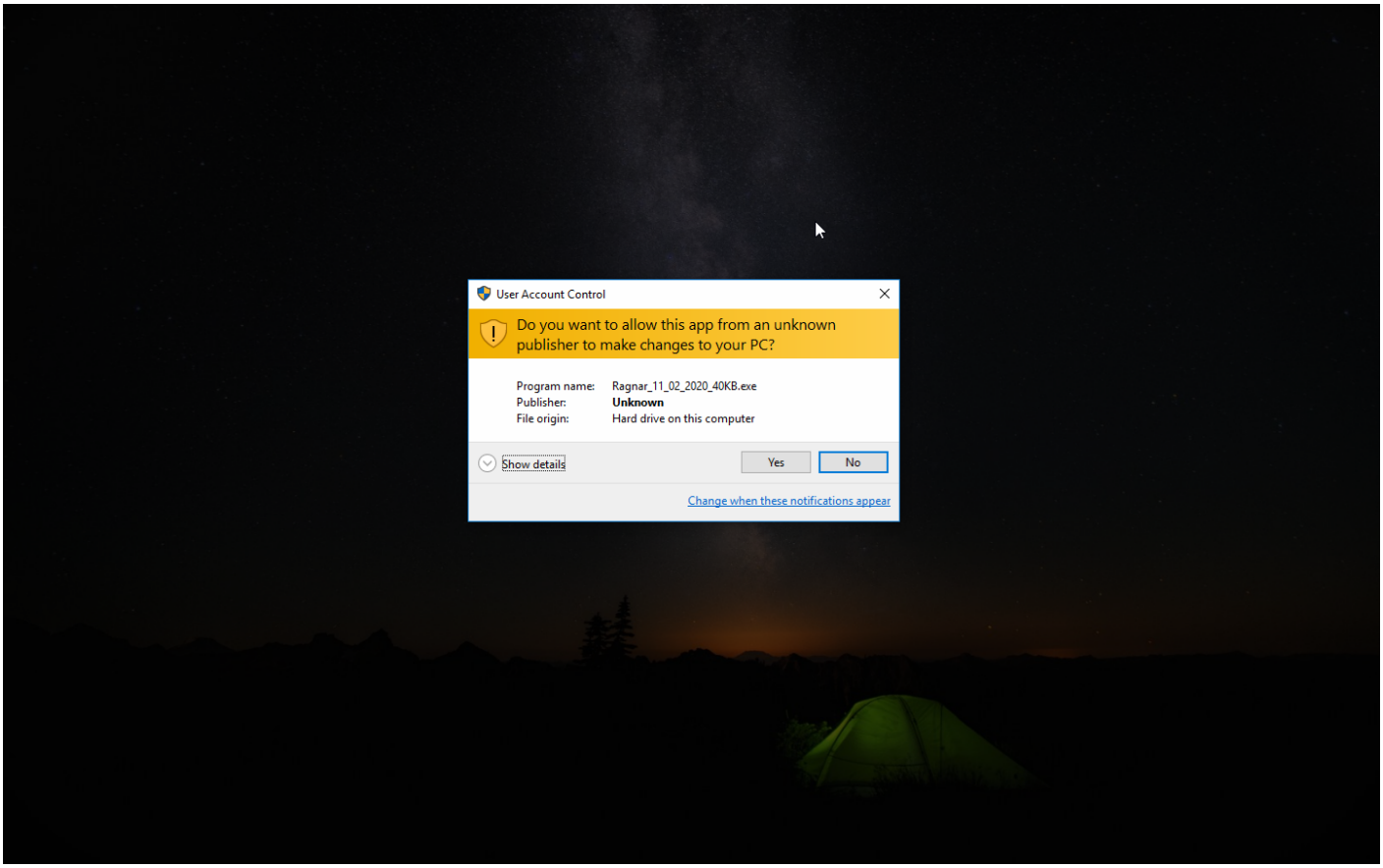
Sample Information

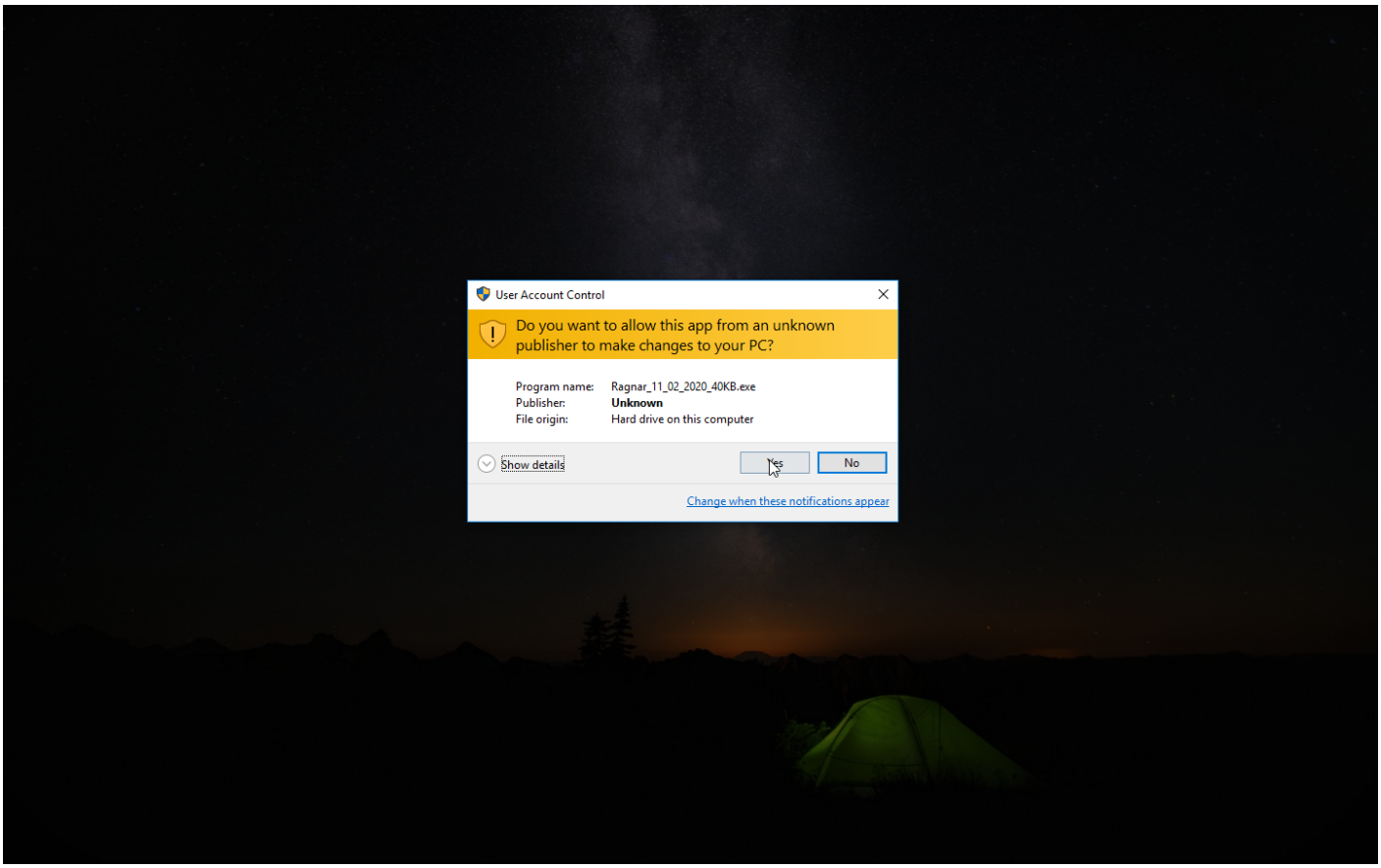
ID	#3193064
MD5	6171000983cf3896d167e0d8aa9b94ba
SHA1	b155264bbfbad7226b5eb3be2ab38c3ecd9f3e18
SHA256	9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376
SSDeep	768:spCmKJILjsoq65corBjd/3oqab0k3RLKul1FX8xUtE:splco4aFoqaXpTX8xa
ImpHash	6a3e7314bd4201552084c30fb976959e
File Name	Ragnar_11_02_2020_40KB.exe
File Size	39.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

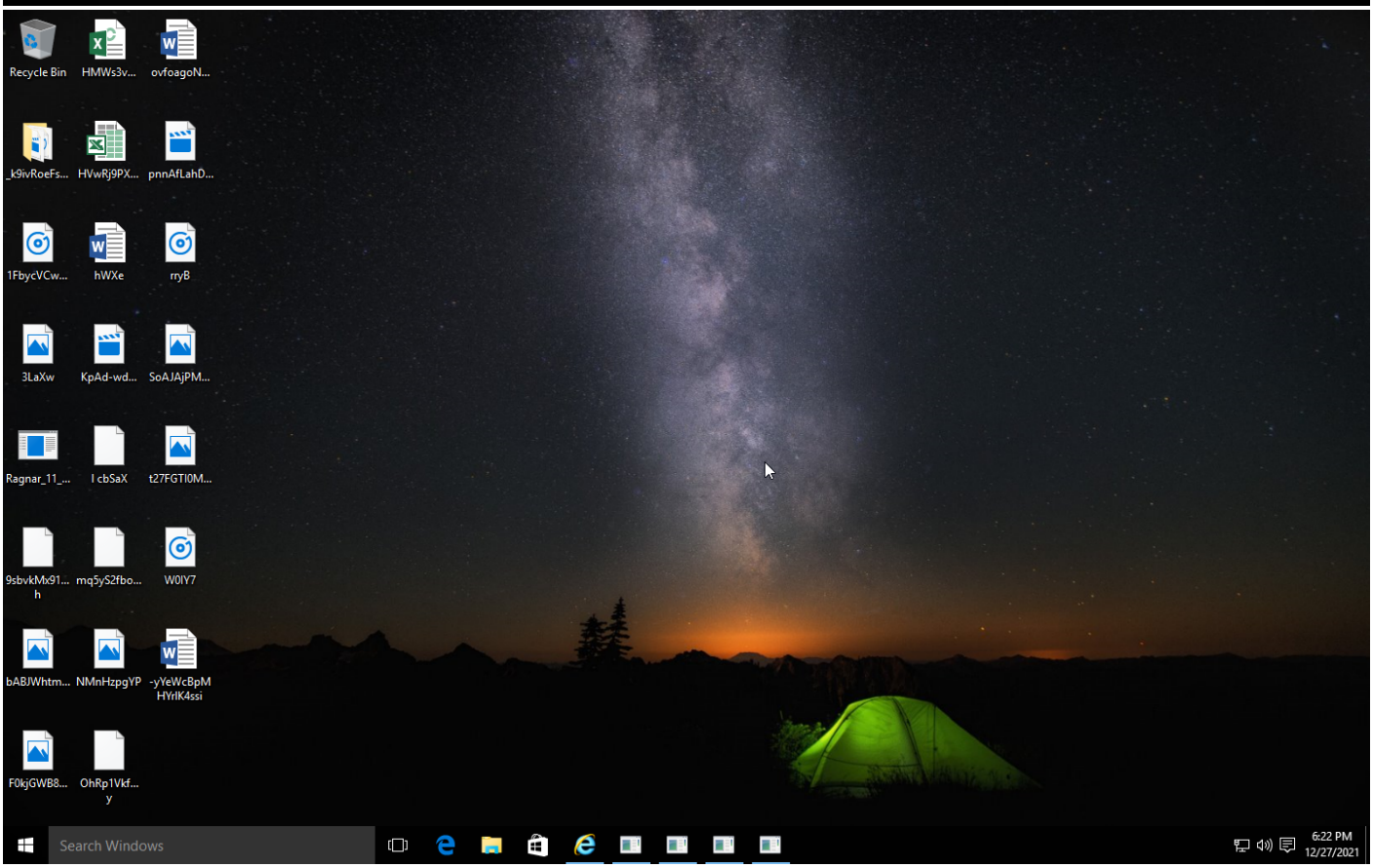
Analysis Information

Creation Time	2021-12-27 19:21 (UTC+1)
Analysis Duration	00:02:41
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	3
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	143


Recycle Bin
HMWs3v...
ovfoagoN...
_k9ivRoeFs...
HVwRj9PX...
pnnAfLahD...
1FbycVCw...
hWXe
rryB
3LaXw
KpAd-wd...
SoAJAjPM...
Ragnar_11_...
I cbSaX
t27FGTI0M...
9sbvkMx91...h
mq5yS2fbo...
W0lY7
bABJWhtm...
NMnHzpgYP
-yYeWcBpMHYrIK4ssi
F0kjGWB8...
OhRp1Vkf...y
Search Windows
6:22 PM
12/27/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: Ragnar_11_02_2020_40KB.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: Ragnar_11_02_2020_40KB.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
HMWs3v...
ovfoagoN...
_k9ivRoeFs...
HVwRj9PX...
pnnAfLahD...
1FbycVCw...
hWXe
rryB
3LaXw
KpAd-wd...
SoAJAjPM...
Ragnar_11_...
I cbSaX
t27FGTI0M...
9sbvkMx91...h
mq5yS2fbo...
W0IY7
bABJWhtm...
NMnHzpgYP
-yYeWcBpMHYrIK4ssi
F0kjGWB8...
OhRp1Vkf...y
Search Windows
6:22 PM
12/27/2021

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

Process #1: ragnar_11_02_2020_40kb.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\ragnar_11_02_2020_40kb.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Ragnar_11_02_2020_40KB.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72299, Reason: Analysis Target
Unmonitor End Time	End Time: 233953, Reason: Terminated by Timeout
Monitor duration	161.65s
Return Code	Unknown
PID	3580
Parent PID	1560
Bitness	32 Bit

Dropped Files (140)

File Name	File Size	SHA256	YARA Match
C:\Users\Public\Documents\RGNR_EEDCF512.txt	3.84 KB	11d42766b1cb0b76e7d3d040ddd90ea8243992145d831852b277e3b0d670f1e0	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\Document Themes 16\Slice.thmx	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
\\?\C:\Boot\BOOTSTAT.DAT	64.51 KB	df62301d39568eb92f4a9057887e6861ba0f8c53d0f7421ef87d3d41d747b894	✗
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml	4.55 KB	c0c674d3f49724dae13e9cf1f5a69df7c1e72bc3377bc32c69ebbc5dffe317eb	✗
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash	623 bytes	6d271c522264b54ea9ae5f0e96ad0398c610bd7106e0494915b8424c8030d2e3	✗
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash	623 bytes	9e4d644ad9d17e7b3988691ef4f700425de259584c3cf8d26a9f7ad9420540b2	✗
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml	5.18 KB	c9fe1f2fbaeb9d2d4c6b80909c7204eb4f75c0d8714f457e2ce3584d0ba92816	✗
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml	4.85 KB	b81df8c96558a8a3a4989236f914283bae42f6f0da2051f17f17ffe959375bbd	✗
\\?\C:\Program Files\Common Files\g8zbElxadWk.bmp	46.13 KB	97936065c950732a9e9008354509d82c701a1b5cc1b487bd278dadc4521ced2a	✗
\\?\C:\Program Files\Common Files\mFNPUwcV_x85.gif	27.25 KB	d4589a22a6d7c3d38d4860e9e525b233ee3aaedcb14b5e62af527a2c7ff38e74	✗
\\?\C:\Program Files\Common Files\rgH4x0V6Uom.png	89.36 KB	09df996d709083518e952e1b05f2ff11fadec3b4503d1d02363a7daa6d85bb77	✗
\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets	5.12 KB	7fae16b1d8b22eb940f073c03b728efce23d463a9f2f51423a9938b5914ab1b8	✗
\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets	5.57 KB	166196d8606846c96e061d68931933dbdb01f1178746e270b2f882c00b373483	✗
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	7.47 KB	20194e162ad6afeba93e3b634c39d0af74623c66d41b68b935854b4e3eaf56b4	✗
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml	3.03 KB	0a477e06e9d35826524bd541a52d79fb447a68445684c4593bcc18fda5c114c2	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml	5.43 KB	4abd3d89d2a1e9821978f8dcf00188ed25882430f769ff9427c4deda04c23571	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	2.00 KB	2a025e83d08be36d409dd7667bb32ac89cbff26772fc0dd35d1a5c74efe578b6	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1	8.12 KB	076bfaec138ca976f0ae367692c97d0a07dae2abcd1308ef1f86a0b7bd84d9bb	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1	78.38 KB	b53cd1e3174eba251d069d7a76e546da6c24df21b48c8c5b669294a6a44a75e7	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	23.20 KB	feee59fcfb103aeaea2994f832ba156c3befdf99a3af14b2f6e0050d969535a5	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	17.96 KB	6fdabfd11a273deb3e6bc53d4dc8991168f7bf790f28361560c1ff7dbd107660	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	81.46 KB	d6095854184348a0d01f5e839850de4261d513f90eaead2e541d373fa89409f9	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	467.20 KB	9985a2ec90d906d6a515a457e91e404b660e7c11899c6c0eee6e38e13c9d84bf	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	1.23 KB	bbd93866403b11c624685d832d67775975176f720469f04edf2f43bee6543f86	✗
\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1	701 bytes	f83792dd7817d29a709e6c08ec679b8d0373b7902fa507f0ad9929356e2f8e8b	✗
\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	16.12 KB	bc4e63b43d0d7ff6e1f346941e2040efe266cf52e7a532475a79e5b455560b71	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	577.19 KB	cb0bac0cb97c77c92a3b16f5b2164f1c66e35171ad886e1a31badc7bb7936412	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store	9.94 KB	612fe7f991c6d010cf718cc78bbc0937fb91fdd4af23966acea2e43f72c094ee	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store	127.95 KB	1ec03815fef68b18fd6493864868d7fc8b39c759495f93d59cd79416a8e3bcbc	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat	89.45 KB	049b71ca6f177b3b3e457e9cd0ec2e313f1bd0f4059ffe6f45f4d23f43f65182	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd	656 bytes	1fa8576404c9c5d827238cbae5f74db0c63f31fccc1f87dd517ab0764ddb1cdf	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb	16.66 KB	f7d604b3a8ef92f44fdd4f556e0fae5bf927e54a9186413e4f8d83075f5262eb	✗
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb	21.65 KB	f052459e89e3bd43170540178a6afde0fdb46817b54419e9bd12c5ed24cae384	✗
\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM	170.95 KB	e4c95267aae0f22685bb25c5261e42789e9074d14d286794fa4f2ef165e18a69	✗
\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS	92.76 KB	fba7701a0b0f50c47877beeefcbe6a4a4961967b1b250aed47c87c0054f536f8	✗
\\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML	35.99 KB	51447dfd1781f23c984a33184a2ac89b220c48cf2907fa8a61f0f6bedba83590	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	315.08 KB	84ed1ef98090cdc54aba580caed77b296fdd006f5a46fa2e518048b9245124a5	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	2.01 KB	c5168368dd91df2eb680899f2891f6556de4ac7a2edd0cc6264c01380c9cb4bc	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	758.40 KB	8e5ebb24a2d1e5205cec3dfe0b7d28938d5b16b9aa75b7ff428aa4d1e7d08c50	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml	1.74 KB	7282590bc89025ddfa67cffbc8c95945c1e44d49053919ff04250a4d0dd31470	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml	453.61 KB	7859417be276d966789a81835bdcb0b915a4800e798ce9449030cca931f1545d	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml	1.74 KB	873c296a9feb4d79818634b4bc68dba082c1886f35fa694427f070625ffb0e79	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml	248.27 KB	259c3349804568bfabf57f3ded8b6e34fdd4e0845ec8f5f8d231a6fadf66b281	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml	1.74 KB	f4f909c01540e010118a8403e134a6c6bc666ec14f022ab5683982a5565cd7c4	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml	1099.08 KB	c018a5f1d0f9939fb4aa2a8d535f73e05b3de2081b61ee77a29eb7e38759d6e6	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	19.50 KB	fc99421cdc68191c2644029730f71811cf20c90b96f8f37b4c3074d89daee166	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml	721.10 KB	59423d4b9a9643f038c755c915780cc8804241dc5d7c826b625524077d88c34f	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml	1.74 KB	c2bdfb66ad8ee2654840f83d3be81f7e72fa2e8626eae99e4546045a03a59dcc	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml	1.74 KB	6103e9c7f25df03bd6a30a35ce4244a4525087b1205fdf637ac1ca6ae45a4c94	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml	2.61 KB	9a300bd0d387a11fd336b8c32f3f2036b50fd448af42774c62352e23b5695357	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	2.61 KB	139eea45c429e94b0a929b661263039e192df78505bcfe74a309a9ad92f976d2	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml	34.39 KB	4b90d2f3e8b0fd0b6f31c13a520fcb58ed11cc16429110ff41f18c76b82441e5	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml	1.74 KB	2889295c7033d3ae8b10c9fb9dd9a22657f175380f94cc5e3c9506400bcd9d01	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	1.74 KB	b06c2352fcaa07adabd6e243e3704ca819f091b1ce166786a1bc3634016ad19b	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml	14.73 KB	32b1972dd7ac23a34ba8e5fd593f62fe6f38bac4a5ecdf6b80fa033466d2358e	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml	349.45 KB	31ad09883fc34a93fe7a1c61279149f5e7fde2ab4a942d223a8fcde1ec7d9003	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml	1.74 KB	4df37c72fceb7a3116bfff33c985d14f368653dd114334b9e2a14221c993d258	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml	55.17 KB	810e67e22caa79f4e78f456e87694a777212f6c8365b8c082012b95fb41890fc	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml	1.74 KB	a837de935ff36a20fb7db5a0a07b7db0fad831b497547e81ecbf966a40884fdc	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml	9.51 KB	118c2c8d6eabfb294731626a0389b5e7bb47345541abebcef21ff84e5d31a791	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml	1.74 KB	12f8cdff3609a16fb79b6acb9a2f7765659cc69b3f9db96f00a6174a86fcd38d	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml	1.92 KB	f35d925e5bd6598f18db6d5fcdd2432c74ea9be3dc9237b7bb7d9938755ed0f6	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml	1.74 KB	570efbc0d09eaaf4dcf73d774e388fc8750a3c49387f31db2f682ac86e50db15	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	4.17 KB	37ea57085e8e0ba7f58c12b97739b06842dab2cf9627e32499044ec3f7797dcb	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml	1.74 KB	cd9d15b4ba0391c15a5b43b1400e70af4e49dca463a93aacc7eab4bef765c9e4	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	1.74 KB	6aa3356cf9fd1f0fa1aad21f4568c312fac43058a7f3d6d214f7388fa77c554d	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml	1.74 KB	9d5802aaa55d4160078dbdf2efe57796c6cd282bf6104f6b28e4376ac61443a5	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml	1.74 KB	d82d5b67a32191359fbe1f90a5b96c3c6c0bd15e86fa89693f6a40eeda7d238e	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml	516.79 KB	399eeebed631bcac647a2ca16599fc525e789e5ccf9bbea947b24701652e6be4	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	1.74 KB	2c76f1b664bf6ec7f80b6c5d9b803da2cdd84f1b4799932b00cfd7e3ec2e6469	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	3.80 KB	4a281cb6e4bf10bd59ff8054d0e67175ae7d8e96dbe7829943164315da883221	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml	1951.49 KB	11be8880cb45fc40f53f0f813781a77efc0cb1f60fefab6861bc0ff4d9a7b8af	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml	10.11 KB	43f9ea60b440fbb6b35b962744a58d53eabfbddbbffd193de4d16972071336c0	✗
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml	894 bytes	b3d1db63761b46fd424db469ca3aa02216b5fc094ee1e2a1626bfb4383dfe346	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF	9.32 KB	8956032aa73fcaa2ea214e4a3cef41ad60682c6bf0a02131a8e61aa75a426ec7	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	7.56 KB	892fc757c457d0b69eadadd3d5ddd77d7b6a27e3c5349ff15ee9de940d467b8e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF	15.03 KB	2589079f8ec0fe021adc39626ab015efb018812a2c72e907945e3774020d6424	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	7.04 KB	fdc848a3dfa188567af80d5e444e8890e06d6b6a5f1c8505c15d55cb624324db	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF	3.68 KB	07a39e99c69130a57e822c864fe436041b3885a373e772239362b4c0a8a58bc4	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF	8.42 KB	8dfe8792a1595fc3542fe122ab5c4a12a887edf282e14cd64b5c8d71822fd5ad	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF	8.01 KB	f41889fa38b44c31b88ca91cbae709ff74b40a359ec6e36da2332e04cb506744	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF	12.12 KB	fdb6f7b51f461a4fec1f7508872ce7cd97c9197be111c645365a86c29bdfb546	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF	1.01 KB	813dc7c23755f51adfa47b9874800f6b3429b69fdc527efe18fdf67b5af2f30c	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF	1023 bytes	bb746b13a74749f0f22ec49fb269d1708929150cad99dc2aa74f4ac993e0ce31	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	12.91 KB	c3bcd2ab8917753b807d13df765fa4c9ec65fe1c2b112b2116784e687a447687	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF	3.91 KB	8f97deaaf41f704fd2a3e49e2d626897570ecf406659e75b14ef3efbbd866267	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF	3.58 KB	fbd9f8c2a120e4ff4f3f459afc7e5d60cefbb41711b55c0e67a2e8c6a0a28dd4	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF	12.70 KB	27cd1f71421e21cd48ebba48d824e2d7e7f3aa4194031fa1afd6bb40e3347f4e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	5.64 KB	2c09553a66de520406e63f74ce22bd4b2bb3e147308dd73d149847996b05809a	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF	3.04 KB	f291ce694d3a8e8baaa8bd85d88a752bb5277861e8c862ebc34583710cd2ba32	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF	10.87 KB	ac09e3c04ac2c639174616c097b00fd2dc6f93d17d87cd0019fbb0aab75aa5ed	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	15.46 KB	58e19b4e2aaa00337dab343f9ad87e908a12225577b4429512db4f814077db49	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF	5.70 KB	38d7d9750dc8c5366de7e6e33a4433cd1d0525b762e5c5a1bbb9cbccbab0c254	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF	5.35 KB	194ec797d42a32c92274ac4a76d8d476ba4b1967e1c681a0989fbf0aa89fa3d1	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF	5.42 KB	f7f20bc92655a03db7cbf290af0623e5a81a47d3563528164ff4438c055479ae	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF	1.63 KB	d42411dd9204b5d44d27bb08f82ac28f4776c5cf35d1506900ccf9c079c7aeca	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF	7.91 KB	3fa3cfa5d50c64d558c818f1d6cef011b9a53560d55316b0f1bfbdbc8a91e36c	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF	7.33 KB	3943d8b35e3703e6391862fd1e552ddaccddd5a325a2d8efec976d9dda19e909	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF	13.45 KB	d3f4e2644c8030ce243940c8c3777ec71144e6620604b333c5c2523f2175046a	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF	8.89 KB	35813c1f710910abb7ed69c92c0ee3b26d098d69099b17fb5524d99fdc221f3e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF	5.29 KB	bc8cd06b7d7722b1f38590bd2eece82d620568da5235e112e352d1791095949e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	5.76 KB	9c894de956ed9506e245ad5c8414c5747e940fe0300b6c2d4db887e58c48b5e4	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	9.54 KB	3da245bd2b0c7eeb6101dd5cf9c80556f79fffaf31cf073824140c32ef29d75e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF	5.41 KB	a8d97e4a808443f6f1bef4462df69b43a999743a1a0b1539861171944e6ded06	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF	4.80 KB	627ed8681888a4ff4daaa3e18bd0d5c0c24c4d1f729f86cc552aa536f109a036	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF	4.38 KB	3660ab7d8123b92b1d426c9a72a6025dfe24156254d5a7402fb8eb449e437ef0	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF	3.81 KB	5f2626a657e15ffc7c65c8203111404e6752ca5ba08a8f33e593c8bb5da49a85	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF	3.56 KB	e190975f634c55389ca4902e5be87daddad01c522936f6ceb13c018950f72890	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF	3.46 KB	7500dc9eff882f9b937033cd45b896329df173f82b633d1dca1c54d3652ab1a3	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	5.13 KB	c97d9a4e10477b877171701f74cd62f0ec6b53a988f8f8efe9ed832f37c889ef	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	6.06 KB	05676f5950f70856b8b6c9ce4b8de14717bd57d510a4af297bcf4d1b97558dcc	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00853_.WMF	20.60 KB	9004c1ed39008cf63673d47e733055ee72176d7798d6afab006e44927e010db7	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00914_.WMF	11.09 KB	4f52dfe5cae328a7fe0cc3d696bba26581964f3e67d489a3d230e12edd43da6c	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00932_.WMF	14.60 KB	1acd8274e5760d34b9bb82997e63394036fe5b5a12d8889f6d0841953a17975f	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00965_.WMF	7.42 KB	8b54f6238b17b0b70fede027df6b48a3ebd7656edc9f91145961c38094497062	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01039_.WMF	3.77 KB	768f8cf99cd4fe19a506ce0a54583e7eb4b6256fd0b12457311907fd34b34a0e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01044_.WMF	2.07 KB	59bb53d3a22bc4baf2bdc78a5500cac21b47cc4fc10821e2a6ff17a5f897da88	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01060_.WMF	8.29 KB	b66c4201b37928819741d5f95bd19407fa5dd842ad28257a82fdcb18f9e6bfad	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01084_.WMF	2.30 KB	a6066968474384d23702709c81622805960ec3031c3d8ab6a6307471a27f81c6	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01173_.WMF	26.22 KB	a13e45e66967700f8042be77d688bef876a81bb7af2662be735b5500c18f40bc	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01174_.WMF	27.71 KB	32772f711082f75f5cf5178236b31107b0625fc423c6ad9417028dcce2bc0766	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01184_.WMF	4.17 KB	d5cc6595303cc376c03216779849836fe1a2ceea1e92de761807e85e44d978c0	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01216_.WMF	6.21 KB	d9e2096cbb0f15db890cba907d57adb4f38d350e9270dbd62768f123dfa69b4e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01218_.WMF	3.45 KB	79cad12a41a64d62a39f3f060655275880b349b32823ccfff211570dc1d851c0	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01251_.WMF	3.20 KB	143c8def2d62ed73fa210c9da1902654148f90cdf36c56f54aa7a2467ac37c1b	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF	7.71 KB	b00505a946ef296a7c679d88702a35919d93ff956014698a209131a566765ea8	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02122_.WMF	7.87 KB	b469084a37a6077c5b5ad85e31f46bfbe903cd41f6760a82c5b1dc8cfd659e55	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02559_.WMF	6.99 KB	d953fe9a1b5c31dc7c576a710f9ab43c4251d621dc5a2a1e886e1be67cb6dbd9	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02724_.WMF	2.57 KB	7fc29dcc97769af77f3cd0f3288c1f5b549bb81be5fb9f780f2602246a47ea5a	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN03500_.WMF	9.53 KB	545b5b47ac8568d8c27bd3b97a3cd5dcc5e95540ddebbe37e28e7596573fad9c	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04108_.WMF	2.80 KB	b3bfc25762e237132269795da135b5b3cc4f9d52f34dd2a9fc5ad05590890c4e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04117_.WMF	6.43 KB	7154331ee7322192d9c3bac881b1c0550f73bb46deadc515ee46146a1bf1d193	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04134_.WMF	3.84 KB	523432e28851cb052df43eccc1777ddf1d2e7f2152a71c481d67cd83c9e2c3c7	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04174_.WMF	3.08 KB	68031df3d3193dddd474c0933413408c191bc89e5375965884d01c746c4d9cec	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04191_.WMF	6.99 KB	ae6575e7eab30b16627664e0bf0c5e426e217c01681c11398b3a5628f1d1dc82	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04195_.WMF	5.01 KB	8417076c9d7da3ae0cef5fa602a4e38f5d200635c53cb43010c7a8637703056f	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04196_.WMF	3.58 KB	0b90ae6fed96ed115974277eff7ffb3f427cc71b92b96218cd5832d164fe180c	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04206_.WMF	8.00 KB	01513242e7cb2cb6fa9262d97f848398cf1244eef484d34afb69e270da844f12	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04225_.WMF	8.80 KB	f5e3ec5b252b57fda6aec32d154c20dd182538fa0655c19e78c4f24908326e5e	✗
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04235_.WMF	8.13 KB	0f70ab9d44c22e64fa5db43aa517d9b7d3e9f8b765c4779a3d80b04b56d680d3	✗

Host Behavior

Type	Count
System	4
User	1
Registry	4
-	1
File	28914
-	2
-	7
Module	4
Process	2

Process #2: wmic.exe

ID	2
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	wmic.exe shadowcopy delete
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96519, Reason: Child Process
Unmonitor End Time	End Time: 129023, Reason: Terminated
Monitor duration	32.50s
Return Code	2147749908
PID	2028
Parent PID	3580
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
COM	3
System	3
Registry	5
File	2
-	1

Process #3: vssadmin.exe

ID	3
File Name	c:\windows\system32\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96933, Reason: Child Process
Unmonitor End Time	End Time: 115712, Reason: Terminated
Monitor duration	18.78s
Return Code	2
PID	3116
Parent PID	3580
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9bdd7f965d1c67396afb0a84c78b4d12118ff377db7efdca4a1340933120f376	C:\Users\RDhJ0CNFevzX\Desktop\Ragnar_11_02_2020_40KB.exe	Sample File	39.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
df62301d39568eb92f4a9057887e6861ba0f8c53d0f7421ef87d3d41d747b894	\\?\C:\Boot\BOOTSTAT.DAT.ragnar_EEDCF512, \\?\C:\Boot\BOOTSTAT.DAT	Modified File	64.51 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c0c674d3f49724dae13e9cf1f5a69df7c1e72bc3377bc32c69ebbc5dffe317eb	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml.ragnar_EEDCF512, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml	Modified File	4.55 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
6d271c522264b54ea9ae5f0e96ad0398c610bd7106e0494915b8424c8030d2e3	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash.ragnar_EEDCF512, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash	Modified File	623 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
9e4d644ad9d17e7b3988691ef4f700425de259584c3cf8d26a9f7ad9420540b2	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash.ragnar_EEDCF512, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash	Modified File	623 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c9fe1f2fbaeb9d2d4c6b80909c7204eb4f75c0d8714f457e2ce3584d0ba92816	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml.ragnar_EEDCF512	Modified File	5.18 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
b81df8c96558a8a3a4989236f914283bae42f6f0da2051f17f17ffe959375bbd	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml.ragnar_EEDCF512, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml	Modified File	4.85 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
97936065c950732a9e9008354509d82c701a1b5cc1b487bd278dadc4521ced2a	\\?\C:\Program Files\Common Files\g8zbElxadWk.bmp.ragnar_EEDCF512, \\?\C:\Program Files\Common Files\g8zbElxadWk.bmp	Modified File	46.13 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d4589a22a6d7c3d38d4860e9e525b233ee3aaedcb14b5e62af527a2c7ff38e74	\\?\C:\Program Files\Common Files\mFNPUwcV_x85.gif, \\?\C:\Program Files\Common Files\mFNPUwcV_x85.gif.ragnar_EEDCF512	Modified File	27.25 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
09df996d709083518e952e1b05f2ff11fadec3b4503d1d02363a7daa6d85bb77	\\?\C:\Program Files\Common Files\rgH4x0V6Uom.png, \\?\C:\Program Files\Common Files\rgH4x0V6Uom.png.ragnar_EEDCF512	Modified File	89.36 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
7fae16b1d8b22eb940f073c03b728efce23d463a9f2f51423a9938b5914ab1b8	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets.ragnar_EEDCF512, \\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets	Modified File	5.12 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
166196d8606846c96e061d68931933dbdb01f1178746e270b2f882c00b373483	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets.ragnar_EEDCF512, \\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets	Modified File	5.57 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
20194e162ad6afeba93e3b634c39d0af74623c66d41b68b935854b4e3eaf56b4	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml.ragnar_EEDCF512, \\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	Modified File	7.47 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
0a477e06e9d35826524bd541a52d79fb447a68445684c4593bcc18fda5c114c2	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml.ragnar_EEDCF512, \\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml	Modified File	3.03 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
4abd3d89d2a1e9821978f8dcf00188ed25882430f769ff9427c4deda04c23571	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml.ragnar_EEDCF512	Modified File	5.43 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
2a025e83d08be36d409dd7667bb32ac89cbff26772fc0dd35d1a5c74efe578b6	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.ragnar_EEDCF512	Modified File	2.00 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
076bfaec138ca976f0ae367692c97d0a07dae2abcd1308ef1f86a0b7bd84d9bb	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1.ragnar_EEDCF512, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1	Modified File	8.12 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
b53cd1e3174eba251d069d7a76e546da6c24df21b48c8c5b669294a6a44a75e7	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1.ragnar_EEDCF512, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1	Modified File	78.38 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
feee59fcfb103aeaea2994f832ba156c3befdf99a3af14b2f6e0050d969535a5	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.ragnar_EEDCF512	Modified File	23.20 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
6fdabfd11a273deb3e6bc53d4dc8991168f7bf790f28361560c1ff7dbd107660	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml.ragnar_EEDCF512, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Modified File	17.96 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d60958541843 48a0d01f5e839850de4261d513f90eaead2e541d373fa89409f9	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1.ragnar_EEDCF512, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Modified File	81.46 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
9985a2ec90d906d6a515a457e91e404b660e7c11899c6c0eee6e38e13c9d84bf	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1.ragnar_EEDCF512	Modified File	467.20 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
bbd93866403b11c624685d832d67775975176f720469f04edf2f43bee6543f86	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1.ragnar_EEDCF512	Modified File	1.23 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f83792dd7817d29a709e6c08ec679b8d0373b7902fa507f0ad9929356e2f8e8b	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1.ragnar_EEDCF512, \\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1	Modified File	701 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
bc4e63b43d0d7ff6e1f346941e2040efe266cf52e7a532475a79e5b455560b71	\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	Modified File	16.12 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
cb0bac0cb97c77c92a3b16f5b2164f1c66e35171ad886e1a31badc7bb7936412	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms.ragnar_EEDCF512	Modified File	577.19 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
612fe7f991c6d010cf718cc78bbc0937fb91fdd4af23966acea2e43f72c094ee	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store	Modified File	9.94 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
1ec03815fef68b18fd6493864868d7fc8b39c759495f93d59cd79416a8e3bcbc	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store	Modified File	127.95 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
049b71ca6f177b3b3e457e9cd0ec2e313f1bd0f4059ffe6f45f4d23f43f65182	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat	Modified File	89.45 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
1fa8576404c9c5d827238cbae5f74db0c63f31fccc1f87dd517ab0764ddb1cdf	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd	Modified File	656 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f7d604b3a8ef92f44fdd4f556e0fae5bf927e54a9186413e4f8d83075f5262eb	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb	Modified File	16.66 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f052459e89e3bd43170540178a6afde0fdb46817b54419e9bd12c5ed24cae384	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb.ragnar_EEDCF512	Modified File	21.65 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
e4c95267aae0f22685bb25c5261e42789e9074d14d286794fa4f2ef165e18a69	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM, \\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM.ragnar_EEDCF512	Modified File	170.95 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
fba7701a0b0f50c47877beeefcbe6a4a4961967b1b250aed47c87c0054f536f8	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS	Modified File	92.76 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
84ed1ef98090cdc54aba580caed77b296fdd006f5a46fa2e518048b9245124a5	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	Modified File	315.08 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c5168368dd91df2eb680899f2891f6556de4ac7a2edd0cc6264c01380c9cb4bc	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	Modified File	2.01 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
8e5ebb24a2d1e5205cec3dfe0b7d28938d5b16b9aa75b7ff428aa4d1e7d08c50	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	Modified File	758.40 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
7282590bc89025ddfa67cffbc8c95945c1e44d49053919ff04250a4d0dd31470	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
7859417be276d966789a81835bdcb0b915a4800e798ce9449030cca931f1545d	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	453.61 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
873c296a9feb4d79818634b4bc68dba082c1886f35fa694427f070625ffb0e79	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
259c3349804568bfabf57f3ded8b6e34fdd4e0845ec8f5f8d231a6fadf66b281	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	248.27 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f4f909c01540e010118a8403e134a6c6bc666ec14f022ab5683982a5565cd7c4	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c018a5f1d0f9939fb4aa2a8d535f73e05b3de2081b61ee77a29eb7e38759d6e6	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1099.08 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fc99421cdc68191c2644029730f71811cf20c90b96f8f37b4c3074d89daee166	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	Modified File	19.50 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
59423d4b9a9643f038c755c915780cc8804241dc5d7c826b625524077d88c34f	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	721.10 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c2bdfb66ad8ee2654840f83d3be81f7e72fa2e8626eae99e4546045a03a59dcc	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
6103e9c7f25df03bd6a30a35ce4244a4525087b1205fdf637ac1ca6ae45a4c94	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
9a300bd0d387a11fd336b8c32f3f2036b50fd448af42774c62352e23b5695357	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	2.61 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
139eea45c429e94b0a929b661263039e192df78505bcfe74a309a9ad92f976d2	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	Modified File	2.61 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
4b90d2f3e8b0fd0b6f31c13a520fcb58ed11cc16429110ff41f18c76b82441e5	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	34.39 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
2889295c7033d3ae8b10c9fb9dd9a22657f175380f94cc5e3c9506400bcd9d01	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b06c2352fcaa07adabd6e243e3704ca819f091b1ce166786a1bc3634016ad19b	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
32b1972dd7ac23a34ba8e5fd593f62fe6f38bac4a5ecdf6b80fa033466d2358e	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	14.73 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
31ad09883fc34a93fe7a1c61279149f5e7fde2ab4a942d223a8fcde1ec7d9003	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	349.45 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
4df37c72fceb7a3116bfff33c985d14f368653dd114334b9e2a14221c993d258	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
810e67e22caa79f4e78f456e87694a777212f6c8365b8c082012b95fb41890fc	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	55.17 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
a837de935ff36a20fb7db5a0a07b7db0fad831b497547e81ecbf966a40884fdc	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
118c2c8d6eabfb294731626a0389b5e7bb47345541abebcef21ff84e5d31a791	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	9.51 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
12f8cdff3609a16fb79b6acb9a2f7765659cc69b3f9db96f00a6174a86fcd38d	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f35d925e5bd6598f18db6d5fcdd2432c74ea9be3dc9237b7bb7d9938755ed0f6	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.92 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
570efbc0d09eaaf4dcf73d774e388fc8750a3c49387f31db2f682ac86e50db15	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
37ea57085e8e0ba7f58c12b97739b06842dab2cf9627e32499044ec3f7797dcb	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	Modified File	4.17 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
cd9d15b4ba0391c15a5b43b1400e70af4e49dca463a93aacc7eab4bef765c9e4	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
6aa3356cf9fd1f0fa1aad21f4568c312fac43058a7f3d6d214f7388fa77c554d	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
9d5802aaa55d4160078dbdf2efe57796c6cd282bf6104f6b28e4376ac61443a5	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d82d5b67a32191359fbe1f90a5b96c3c6c0bd15e86fa89693f6a40eeda7d238e	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
399eeebed631bcac647a2ca16599fc525e789e5ccf9bbea947b24701652e6be4	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512	Modified File	516.79 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2c76f1b664bf6ec7f80b6c5d9b803da2cdd84f1b4799932b00cfd7e3ec2e6469	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
4a281cb6e4bf10bd59ff8054d0e67175ae7d8e96dbe7829943164315da883221	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	Modified File	3.80 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
11be8880cb45fc40f53f0f813781a77efc0cb1f60fefab6861bc0ff4d9a7b8af	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml	Modified File	1951.49 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
43f9ea60b440fbb6b35b962744a58d53eabfbddbbffd193de4d16972071336c0	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml	Modified File	10.11 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
b3d1db63761b46fd424db469ca3aa02216b5fc094ee1e2a1626bfb4383dfe346	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml	Modified File	894 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
8956032aa73fcaa2ea214e4a3cef41ad60682c6bf0a02131a8e61aa75a426ec7	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF.ragnar_EEDCF512	Modified File	9.32 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
892fc757c457d0b69eadadd3d5ddd77d7b6a27e3c5349ff15ee9de940d467b8e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	Modified File	7.56 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
2589079f8ec0fe021adc39626ab015efb018812a2c72e907945e3774020d6424	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF.ragnar_EEDCF512	Modified File	15.03 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
fdc848a3dfa188567af80d5e444e8890e06d6b6a5f1c8505c15d55cb624324db	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	Modified File	7.04 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
07a39e99c69130a57e822c864fe436041b3885a373e772239362b4c0a8a58bc4	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF	Modified File	3.68 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
8dfe8792a1595fc3542fe122ab5c4a12a887edf282e14cd64b5c8d71822fd5ad	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF	Modified File	8.42 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f41889fa38b44c31b88ca91cbae709ff74b40a359ec6e36da2332e04cb506744	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF.ragnar_EEDCF512	Modified File	8.01 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fdb6f7b51f461a4fec1f7508872ce7cd97c9197be111c645365a86c29bdfb546	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF	Modified File	12.12 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
813dc7c23755f51adfa47b9874800f6b3429b69fdc527efe18fdf67b5af2f30c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF.ragnar_EEDCF512	Modified File	1.01 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
bb746b13a74749f0f22ec49fb269d1708929150cad99dc2aa74f4ac993e0ce31	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF.ragnar_EEDCF512	Modified File	1023 bytes	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
c3bcd2ab8917753b807d13df765fa4c9ec65fe1c2b112b2116784e687a447687	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	Modified File	12.91 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
8f97deaaf41f704fd2a3e49e2d626897570ecf406659e75b14ef3efbbd866267	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF.ragnar_EEDCF512	Modified File	3.91 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
fbd9f8c2a120e4ff4f3f459afc7e5d60cefbb41711b55c0e67a2e8c6a0a28dd4	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF.ragnar_EEDCF512	Modified File	3.58 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
27cd1f71421e21cd48ebba48d824e2d7e7f3aa4194031fa1afd6bb40e3347f4e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF.ragnar_EEDCF512	Modified File	12.70 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
2c09553a66de520406e63f74ce22bd4b2bb3e147308dd73d149847996b05809a	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	Modified File	5.64 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
f291ce694d3a8e8baaa8bd85d88a752bb5277861e8c862ebc34583710cd2ba32	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF	Modified File	3.04 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
ac09e3c04ac2c639174616c097b00fd2dc6f93d17d87cd0019fbb0aab75aa5ed	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF.ragnar_EEDCF512	Modified File	10.87 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
58e19b4e2aaa00337dab343f9ad87e908a12225577b4429512db4f814077db49	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	Modified File	15.46 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
38d7d9750dc8c5366de7e6e33a4433cd1d0525b762e5c5a1bbb9cbccbab0c254	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF.ragnar_EEDCF512	Modified File	5.70 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
194ec797d42a32c92274ac4a76d8d476ba4b1967e1c681a0989fbf0aa89fa3d1	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF.ragnar_EEDCF512	Modified File	5.35 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f7f20bc92655a03db7cbf290af0623e5a81a47d3563528164ff4438c055479ae	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF.ragnar_EEDCF512	Modified File	5.42 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d42411dd9204b5d44d27bb08f82ac28f4776c5cf35d1506900ccf9c079c7aeca	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF.ragnar_EEDCF512	Modified File	1.63 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
3fa3cfa5d50c64d558c818f1d6cef011b9a53560d55316b0f1bfbdbc8a91e36c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF	Modified File	7.91 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
3943d8b35e3703e6391862fd1e552ddaccddd5a325a2d8efec976d9dda19e909	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF	Modified File	7.33 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
d3f4e2644c8030ce243940c8c3777ec71144e6620604b333c5c2523f2175046a	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF.ragnar_EEDCF512	Modified File	13.45 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
35813c1f710910abb7ed69c92c0ee3b26d098d69099b17fb5524d99fdc221f3e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF.ragnar_EEDCF512	Modified File	8.89 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
bc8cd06b7d7722b1f38590bd2eece82d620568da5235e112e352d1791095949e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF.ragnar_EEDCF512	Modified File	5.29 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
9c894de956ed9506e245ad5c8414c5747e940fe0300b6c2d4db887e58c48b5e4	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	Modified File	5.76 KB	application/octet-stream	Delete, Read, Access, Write, Create	MALICIOUS
3da245bd2b0c7eeb6101dd5cf9c80556f79fffaf31cf073824140c32ef29d75e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	Modified File	9.54 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
a8d97e4a808443f6f1bef4462df69b43a999743a1a0b1539861171944e6ded06	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF.ragnar_EEDCF512	Modified File	5.41 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
627ed8681888a4ff4daaa3e18bd0d5c0c24c4d1f729f86cc552aa536f109a036	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF	Modified File	4.80 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
3660ab7d8123b92b1d426c9a72a6025dfe24156254d5a7402fb8eb449e437ef0	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF	Modified File	4.38 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
5f2626a657e15ffc7c65c8203111404e6752ca5ba08a8f33e593c8bb5da49a85	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF	Modified File	3.81 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e190975f634c55389ca4902e5be87daddad01c522936f6ceb13c018950f72890	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF.ragnar_EEDCF512	Modified File	3.56 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
7500dc9eff882f9b937033cd45b896329df173f82b633d1dca1c54d3652ab1a3	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF.ragnar_EEDCF512	Modified File	3.46 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
c97d9a4e10477b877171701f74cd62f0ec6b53a988f8f8efe9ed832f37c889ef	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	Modified File	5.13 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
05676f5950f70856b8b6c9ce4b8de14717bd57d510a4af297bcf4d1b97558dcc	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	Modified File	6.06 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
9004c1ed39008cf63673d47e733055ee72176d7798d6afab006e44927e010db7	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00853_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00853_.WMF.ragnar_EEDCF512	Modified File	20.60 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
4f52dfe5cae328a7fe0cc3d696bba26581964f3e67d489a3d230e12edd43da6c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00914_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00914_.WMF.ragnar_EEDCF512	Modified File	11.09 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
1acd8274e5760d34b9bb82997e63394036fe5b5a12d8889f6d0841953a17975f	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00932_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00932_.WMF.ragnar_EEDCF512	Modified File	14.60 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
8b54f6238b17b0b70fede027df6b48a3ebd7656edc9f91145961c38094497062	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00965_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00965_.WMF	Modified File	7.42 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
768f8cf99cd4fe19a506ce0a54583e7eb4b6256fd0b12457311907fd34b34a0e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01039_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01039_.WMF.ragnar_EEDCF512	Modified File	3.77 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
59bb53d3a22bc4baf2bdc78a5500cac21b47cc4fc10821e2a6ff17a5f897da88	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01044_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01044_.WMF.ragnar_EEDCF512	Modified File	2.07 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
b66c4201b37928819741d5f95bd19407fa5dd842ad28257a82fdcb18f9e6bfad	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01060_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01060_.WMF	Modified File	8.29 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
a6066968474384d23702709c81622805960ec3031c3d8ab6a6307471a27f81c6	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01084_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01084_.WMF.ragnar_EEDCF512	Modified File	2.30 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
a13e45e66967700f8042be77d688bef876a81bb7af2662be735b5500c18f40bc	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01173_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01173_.WMF	Modified File	26.22 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
32772f711082f75f5cf5178236b31107b0625fc423c6ad9417028dcce2bc0766	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01174_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01174_.WMF.ragnar_EEDCF512	Modified File	27.71 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
d5cc6595303cc376c03216779849836fe1a2ceea1e92de761807e85e44d978c0	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01184_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01184_.WMF.ragnar_EEDCF512	Modified File	4.17 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
d9e2096cbb0f15db890cba907d57adb4f38d350e9270dbd62768f123dfa69b4e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01216_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01216_.WMF	Modified File	6.21 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
79cad12a41a64d62a39f3f060655275880b349b32823ccfff211570dc1d851c0	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01218_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01218_.WMF	Modified File	3.45 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
143c8def2d62ed73fa210c9da1902654148f90cdf36c56f54aa7a2467ac37c1b	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01251_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01251_.WMF.ragnar_EEDCF512	Modified File	3.20 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
b00505a946ef296a7c679d88702a35919d93ff956014698a209131a566765ea8	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF.ragnar_EEDCF512	Modified File	7.71 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
b469084a37a6077c5b5ad85e31f46bfbe903cd41f6760a82c5b1dc8cfd659e55	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02122_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02122_.WMF	Modified File	7.87 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
d953fe9a1b5c31dc7c576a710f9ab43c4251d621dc5a2a1e886e1be67cb6dbd9	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02559_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02559_.WMF.ragnar_EEDCF512	Modified File	6.99 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
7fc29dcc97769af77f3cd0f3288c1f5b549bb81be5fb9f780f2602246a47ea5a	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02724_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02724_.WMF	Modified File	2.57 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
545b5b47ac8568d8c27bd3b97a3cd5dcc5e95540ddebbe37e28e7596573fad9c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN03500_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN03500_.WMF.ragnar_EEDCF512	Modified File	9.53 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
b3bfc25762e237132269795da135b5b3cc4f9d52f34dd2a9fc5ad05590890c4e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04108_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04108_.WMF.ragnar_EEDCF512	Modified File	2.80 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
7154331ee7322192d9c3bac881b1c0550f73bb46deadc515ee46146a1bf1d193	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04117_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04117_.WMF	Modified File	6.43 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
523432e28851cb052df43eccc1777ddf1d2e7f2152a71c481d67cd83c9e2c3c7	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04134_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04134_.WMF.ragnar_EEDCF512	Modified File	3.84 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
68031df3d3193dddd474c0933413408c191bc89e5375965884d01c746c4d9cec	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04174_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04174_.WMF.ragnar_EEDCF512	Modified File	3.08 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
ae6575e7eab30b16627664e0bf0c5e426e217c01681c11398b3a5628f1d1dc82	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04191_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04191_.WMF	Modified File	6.99 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
8417076c9d7da3ae0cef5fa602a4e38f5d200635c53cb43010c7a8637703056f	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04195_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04195_.WMF	Modified File	5.01 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
0b90ae6fed96ed115974277eff7ffb3f427cc71b92b96218cd5832d164fe180c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04196_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04196_.WMF.ragnar_EEDCF512	Modified File	3.58 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
01513242e7cb2cb6fa9262d97f848398cf1244eef484d34afb69e270da844f12	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04206_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04206_.WMF.ragnar_EEDCF512	Modified File	8.00 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
f5e3ec5b252b57fda6aec32d154c20dd182538fa0655c19e78c4f24908326e5e	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04225_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04225_.WMF.ragnar_EEDCF512	Modified File	8.80 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
0f70ab9d44c22e64fa5db43aa517d9b7d3e9f8b765c4779a3d80b04b56d680d3	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04235_.WMF.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04235_.WMF	Modified File	8.13 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
51447dfd1781f23c984a33184a2ac89b220c48cf2907fa8a61f0f6bedba83590	\\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML.ragnar_EEDCF512, \\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML	Modified File	35.99 KB	application/octet-stream	Delete, Read, Access, Write, Create	CLEAN
11d42766b1cb0b76e7d3d040ddd90ea8243992145d831852b277e3b0d670f1e0	\\?\C:\Program Files\Common Files\microsoft shared\ink\lv-LV\RGNR_EEDCF512.txt, \\?\C:\Boot\sr-Latn-CS\RGNR_EEDCF512.txt, \\?\C:\P...ommon Files\microsoft shared\ink\LanguageModel\RGNR_EEDCF512.txt, \\?\C:\Program Files\WindowsPowerShell\Modules\RGNR_EEDCF512.txt	Dropped File	3.84 KB	text/plain	Access, Write, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
\\.\PHYSICALDRIVE0	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE1	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE2	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE3	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE4	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE5	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE6	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE7	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\.\PHYSICALDRIVE8	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE9	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE10	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE11	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE12	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE13	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE14	Accessed File	Access	CLEAN
\\.\PHYSICALDRIVE15	Accessed File	Access	CLEAN
C:\Users\Public\Documents\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN
\\?\C:\Boot\bg-BG\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\bg-BG\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\bg-BG\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\cs-CZ\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\cs-CZ\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\cs-CZ\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\cs-CZ\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\cs-CZ\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\da-DK\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\da-DK\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\da-DK\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\da-DK\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\da-DK\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\de-DE\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\de-DE\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\de-DE\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\de-DE\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\de-DE\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\el-GR\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\el-GR\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\el-GR\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\el-GR\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\el-GR\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-GB\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-GB\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\en-GB\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-US\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-US\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\en-US\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-US\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\en-US\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-ES\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-ES\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\es-ES\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-ES\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\es-ES\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-MX\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-MX\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\es-MX\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\et-EE\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\et-EE\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\et-EE\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\fi-FI\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\fi-FI\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\fi-FI\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\fi-FI\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\fi-FI\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\chs_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\chs_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\cht_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\cht_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\jpn_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\jpn_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\kor_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\kor_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\malgunn_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\malgunn_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\malgun_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\malgun_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\meiryon_boot.ttf	Accessed File	Access, Delete	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\Fonts\meiryon_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\meiryo_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\meiryo_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\msjhn_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\msjhn_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\msjh_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\msjh_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\msyhn_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\msyhn_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\msyh_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\msyh_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\segmono_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\segmono_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\segoen_slboot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\segoen_slboot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\segoe_slboot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\segoe_slboot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\wgl4_boot.ttf	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\Fonts\wgl4_boot.ttf.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-CA\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-CA\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\fr-CA\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-FR\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-FR\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\fr-FR\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-FR\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\fr-FR\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\hr-HR\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\hr-HR\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\hr-HR\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\hu-HU\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\hu-HU\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\hu-HU\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\hu-HU\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\hu-HU\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\it-IT\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\it-IT\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\it-IT\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\it-IT\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\it-IT\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\ja-JP\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\ja-JP\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\ja-JP\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\ja-JP\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\ja-JP\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\ko-KR\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\ko-KR\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\ko-KR\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\ko-KR\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\ko-KR\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\lt-LT\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\lt-LT\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\lt-LT\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\lv-LV\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\lv-LV\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\lv-LV\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\nb-NO\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\nb-NO\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\nb-NO\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\nb-NO\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\nb-NO\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\nl-NL\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\nl-NL\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\nl-NL\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\nl-NL\memtest.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\nl-NL\memtest.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\pl-PL\RGNR_EEDCF512.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\pl-PL\bootmgr.exe.mui	Accessed File	Access, Delete	CLEAN
\\?\C:\Boot\pl-PL\bootmgr.exe.mui.ragnar_EEDCF512	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Boot\pl-PL\memtest.exe.mui	Accessed File	Access, Delete	CLEAN

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	ragnar_11_02_2020_40kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	ragnar_11_02_2020_40kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	ragnar_11_02_2020_40kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	ragnar_11_02_2020_40kb.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	read, access	wmic.exe	CLEAN

Process

Process Name	Commandline	Verdict
ragnar_11_02_2020_40kb.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Ragnar_11_02_2020_40KB.exe"	MALICIOUS
wmic.exe	wmic.exe shadowcopy delete	SUSPICIOUS
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN

YARA / AV

YARA (143)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLocker	RagnarLocker Ransomware	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\Ragnar_11_02_2020_40KB.exe	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Boot\BOOTSTAT.DAT	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\g8zbElxadWk.bmp	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\mFNPUwcV_x85.gif	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Common Files\rgH4x0V6Uom.png	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00853_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00914_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00932_.WMF	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00965_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01039_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01044_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01060_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01084_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01173_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01174_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01184_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01216_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01218_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01251_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02122_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02559_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN02724_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN03500_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04108_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04117_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04134_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04174_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04191_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04195_.WMF	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04196_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04206_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04225_.WMF	Ransomware	5/5
Ransomware	RagnarLockerEncryptedFile	File encrypted by RagnarLocker Ransomware	Dropped File	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN04235_.WMF	Ransomware	5/5
Ransomware	RagnarLocker	RagnarLocker Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	RagnarLocker	RagnarLocker Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	RagnarLocker	RagnarLocker Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	RagnarLocker	RagnarLocker Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	RagnarLocker	RagnarLocker Ransomware	Memory Dump	-	Ransomware	5/5

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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
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