MALICIOUS

Classifications: Ransomware

Threat Names: Gibberish, Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe**
ID	#4191630
MD5	2d941c8eaf1965025daba7fbb7be273f
SHA1	c0882260b6070c2eaad116be1113af0ad5b782bb
SHA256	d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9
File Size	204.50 KB
Report Created	2022-04-25 18:14 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 115 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 183 files by appending the extension ".$$$".			
5/5	User Data Modification	Modifies Windows automatic backups	1	-
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe deletes Windows volume shadow copies.			
5/5	YARA	Malicious content matched by YARA rules	1	Ransomware
	• Rule "Gibberish" from ruleset "Ransomware" has matched on a memory dump for (process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe starts (process #2) vssadmin.exe with a hidden window.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe enumerates running processes.			
1/5	Hide Tracks	Changes folder appearance	6	-
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\$recycle.bin\s-1-5-21-1560258661-3990802383-1811730007-1000". • (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\$recycle.bin\s-1-5-18". • (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\program files\common files\microsoft shared\stationery". • (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\program files". • (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\program files (x86)\common files\microsoft shared\stationery". • (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe changes the appearance of folder "c:\program files (x86)".			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\1iz126n_fyjfdzvpi4k_.jpg".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\1iz126n_fyjfdzvpi4k_.jpg.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\appvcleaner.exe".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\appvshnotify.exe".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\appvshnotify.exe.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\integratedoffice.exe".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\appvcleaner.exe.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\mavinject32.exe".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\mavinject32.exe.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\integratedoffice.exe.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\ar-sa\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\cs-cz\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\da-dk\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\de-de\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\el-gr\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\en-gb\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\bg-bg\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\en-us\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\es-es\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\es-mx\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\et-ee\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fi-fi\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fr-ca\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fr-fr\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\auxpad\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\insert\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\keypad\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\main\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskclearui\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskmenu\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\osknav\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\osknumpad\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\oskpred\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officec2rclient.exe.$$$".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\symbols\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\fsdefinitions\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\he-il\readme.txt".
- (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe modifies "c:\program files\common files\microsoft shared\ink\hr-hr\readme.txt".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe resolves 216 API functions by name.			

Mitre ATT&CK Matrix

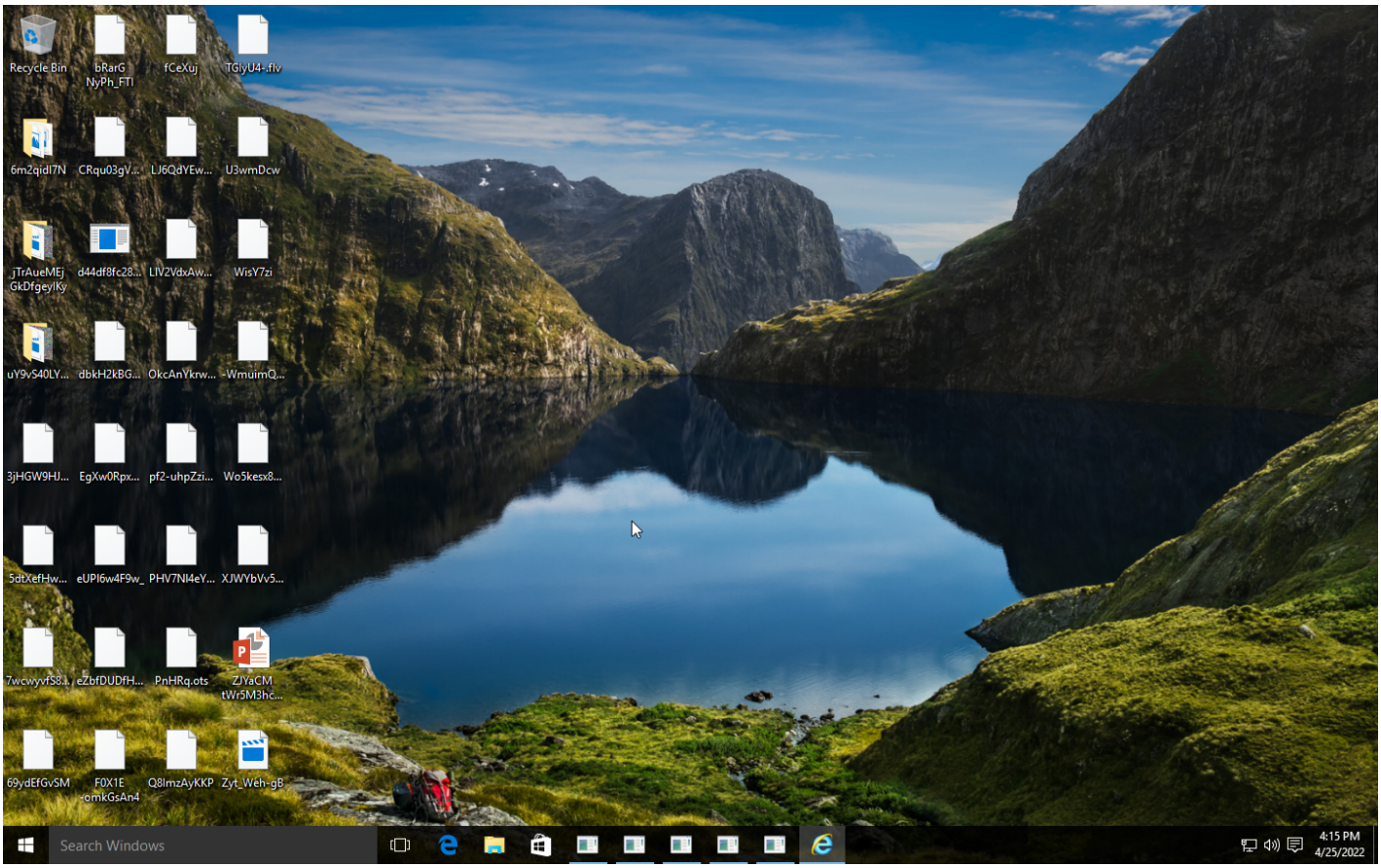
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window		#T1057 Process Discovery					#T1486 Data Encrypted for Impact
				#T1036 Masquerading							#T1490 Inhibit System Recovery
				#T1045 Software Packing							

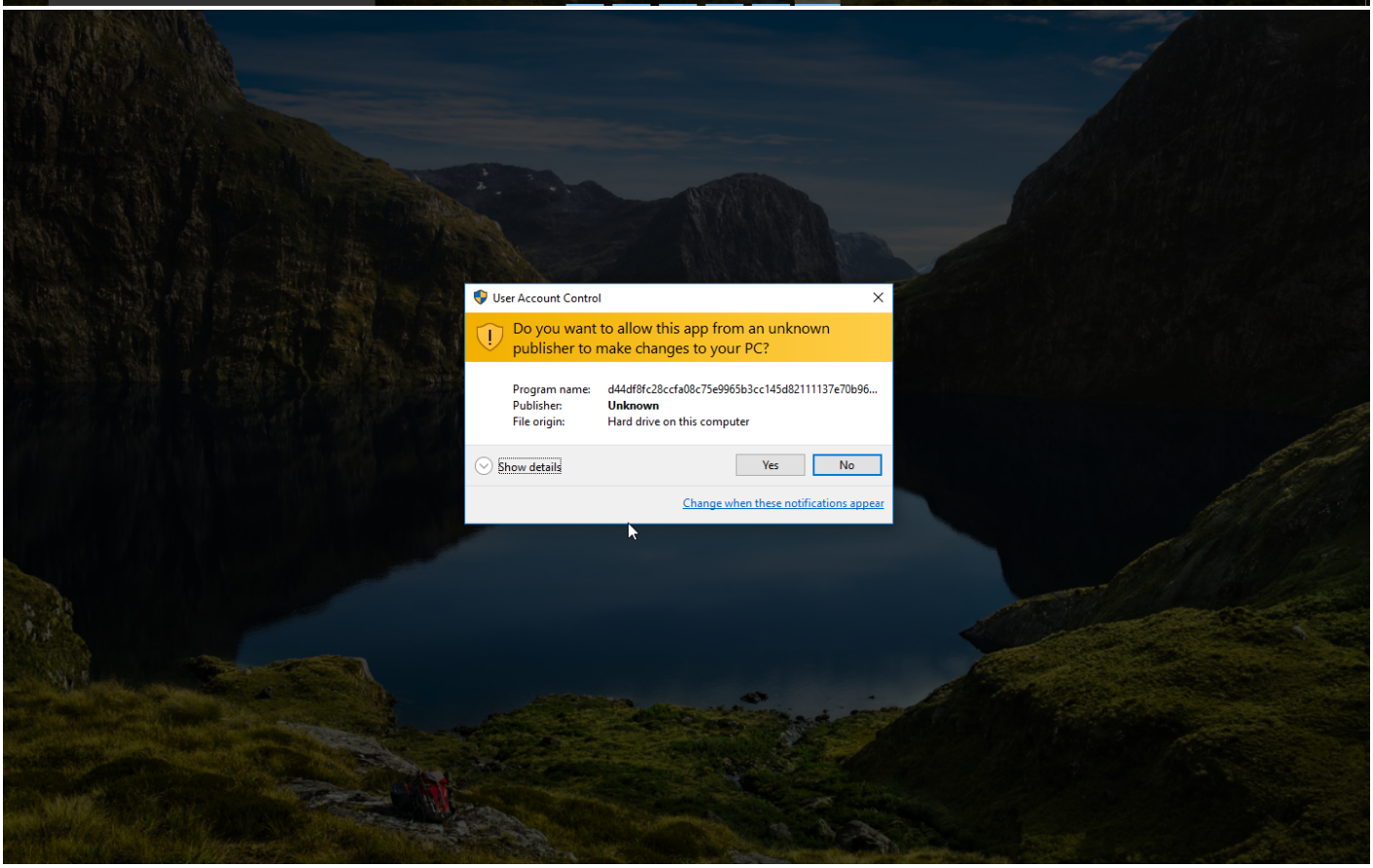
Sample Information

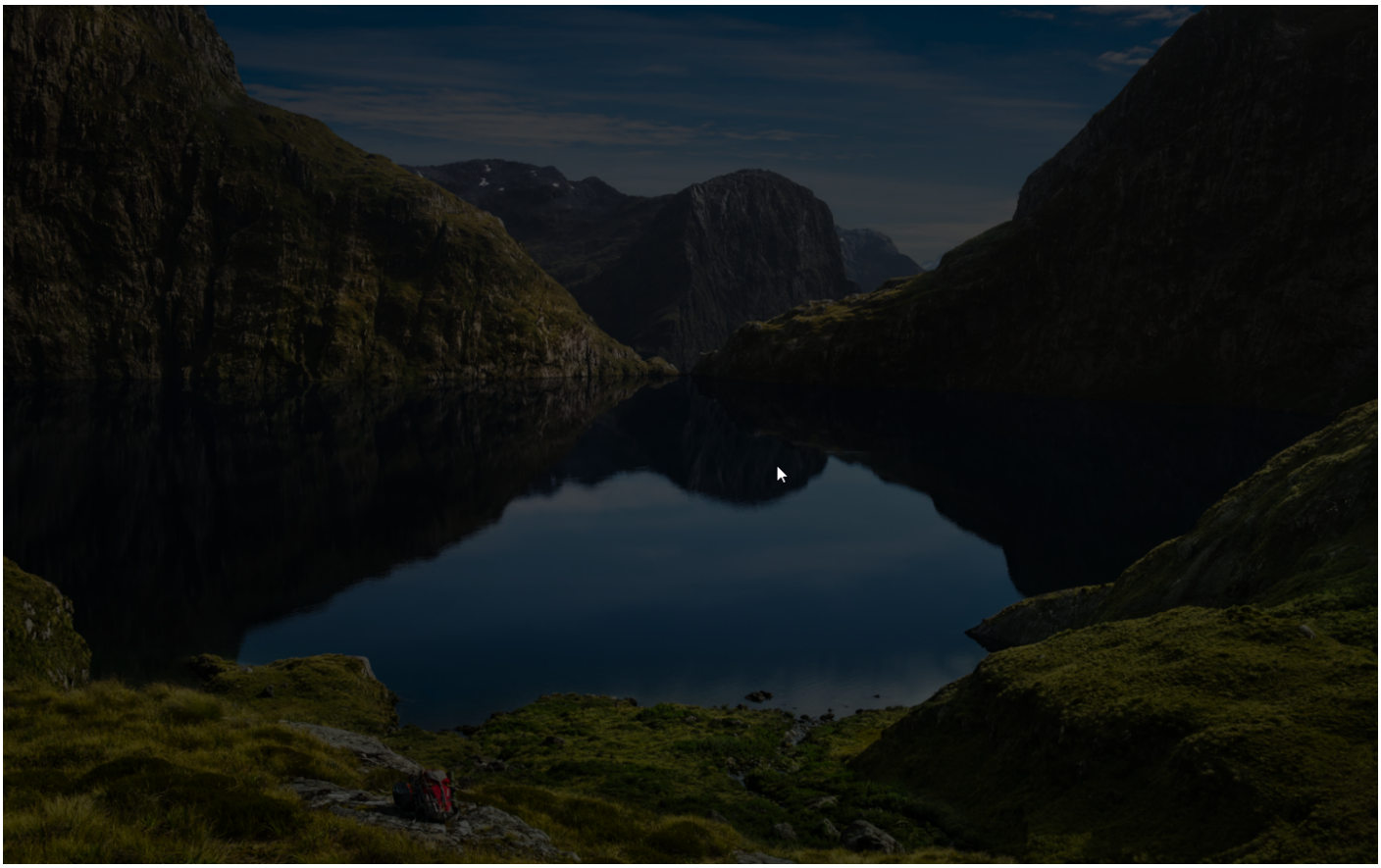
ID	#4191630
MD5	2d941c8eaf1965025daba7fbb7be273f
SHA1	c0882260b6070c2eaad116be1113af0ad5b782bb
SHA256	d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9
SSDeep	3072:RYzZtPvliDxy6Pd1xImk8cOD8quMAvbnnobWmbonnTAdGVJtO7ye5EgvjI:0tPv8xp3lB4D+FnvJnTNJtO+e5Egvk
ImpHash	08e421ba068032c82b323995a63ca93b
File Name	d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe
File Size	204.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

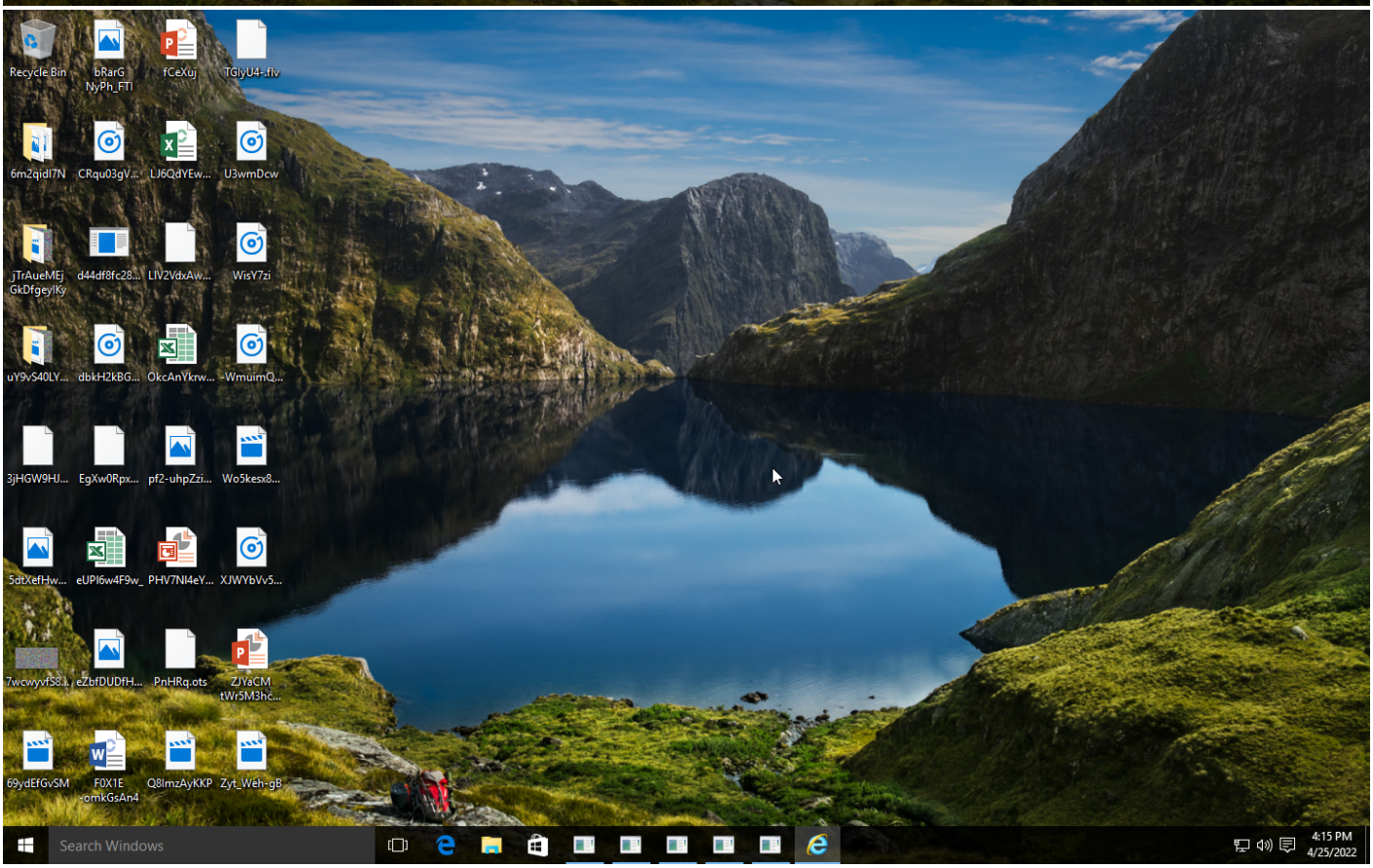
Analysis Information

Creation Time	2022-04-25 18:14 (UTC+2)
Analysis Duration	00:02:13
Termination Reason	Maximum binlog size reached
Number of Monitored Processes	2
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	56


Recycle Bin
bRarG NyPh_FTI
fCeXuj
TGlyU4-.flv
6m2qidl7N
CRqu03gV...
LJ6QdYEw...
U3wmDcw
jTrAueMEj GkDfgeylKy
d44df8fc28...
LIV2VdxAw...
WisY7zi
uY9vS40LY...
dbkH2kBG...
OkcAnYkrw...
-WmuimQ...
3jHGW9HJ...
EgXw0Rpx...
pf2-uhpZzi...
Wo5kesx8...
5dtXefHw...
eUPI6w4F9w_
PHV7NI4eY...
XJWYbVv5...
7wcwyvf38...
eZbfDUDfH...
PnHRq.ots
ZJYaCM tWr5M3hc...
69ydEfGvSM
F0X1E -omkGsAn4
Q8ImzAyKKP
Zyt_Weh-gB
Search Windows
4:15 PM
4/25/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Recycle Bin
bRarG NyPh_FTI
fCeXuj
TGlyU4-flv
6m2qidl7N
CRqu03gV...
LJ6QdYEw...
U3wmDcw
jTrAueMEj GkDfgeylKy
d44df8fc28...
LIV2VdxAw...
WisY7zi
uY9vS40LY...
dbkH2kBG...
OkcAnYkrw...
-WmuimQ...
3jHGW9HJ...
EgXw0Rpx...
pf2-uhpZzi...
Wo5kesx8...
5dtXefHw...
eUPI6w4F9w_
PHV7NI4eY...
XJWYbVv5...
7wcwyvfS8...
eZbfDUDfH...
PnHRq.ots
ZJYaCM tWr5M3hc...
69ydEfGvSM
F0X1E -omkGsAn4
Q8lmzAyKKP
Zyt_Weh-gB
Search Windows
4:15 PM
4/25/2022

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

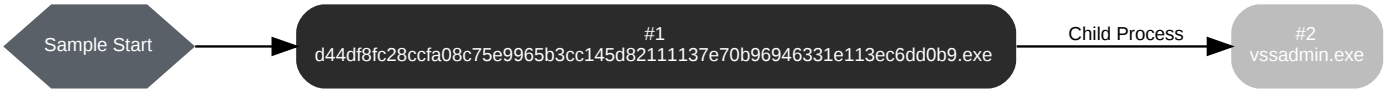
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 82915, Reason: Analysis Target
Unmonitor End Time	End Time: 216976, Reason: Terminated by Timeout
Monitor duration	134.06s
Return Code	Unknown
PID	1908
Parent PID	1184
Bitness	32 Bit

Dropped Files (137)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\readme.txt	438 bytes	4713834aef2c852bbeda1b84a77d14f49877cff0020afca7f74960933e30b0a8	✕
\\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini	649 bytes	63966283db8fd46ddfd282ee59dc6a52e491ccad38662731623f7aeb0df0ca54	✕
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini	649 bytes	1374a958c89c16b852c357bf37a8168e830a355f26198f2003400c612b8cdff3	✕
\\?\C:\Boot\BCD.LOG1	520 bytes	6e748a93fcb3fcb11db0dafc3a2b47e3a00965ef65d5027687648eecdd884fd2	✕
\\?\C:\Boot\BCD.LOG2	520 bytes	fc79424cb7ae039530b4452ca34f387828abe31a7701be1a8ef15e4dc96ff7c3	✕
\\?\C:\Boot\BOOTSTAT.DAT	64.51 KB	8a8d9ea8b99d55a8e9adca68344ca824a82a6ee2151214b18718ea5d25e7dcdb	✕
\\?\C:\BOOTNXT	521 bytes	47662e6faa3e6ffa90c90ee916863fe848b4053b25c7f196aa7667d7b578438a	✕
\\?\C:\Program Files\Common Files\1iz126n_fyjFdzvpI4k_.jpg	55.11 KB	63703222a5b725355360c01c4b6f76d81a4e8736201b0f8bac8b3bde0c40bddc	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\appvcleaner.exe	2007.22 KB	d3110d540fe7516a62049c7e2a4983885b35db04db65768b522538a1200f8afa	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe	258.22 KB	0552f835f097eaf565525870ecf769cffba9c9d20ccc1ba9c6e22652eeea37c4	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml	4.55 KB	0aa1281c57501690bdc25033c15380682af6c982652d2c65b52a979a4d8e7b0b	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash	622 bytes	3efa9efec5533209917390ebaeb68afa697616e7e69f75db1a615ddd5674c2ba	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash	622 bytes	00a73fe811f8097e5894edb82bcf91b3c9b9b6d3f5d4e0cbcf9e197d534c47cd	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\IntegratedOffice.exe	1068.13 KB	7f81a171cc707baf489992f32446cb6ca2a71f2476dd680f9728792ef7f155e3	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe	350.72 KB	2561c07008955e58b0b6127894f3237b7ca13cf41fa3f3fc2641135b1a1ed011	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe	5828.61 KB	62ac6062d10753cc587558d1539e0bb06b982e6086cfe84b701864ec941b9dfb	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml	5.18 KB	600a51b61867ffb565bfd4ec0b1e7fb340dfdb616ede4e87d11301a0a1bebad8	✕
\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml	4.85 KB	24ef368426ce551f33078f9a21958e57e1745d0b64f44574702b65a67d889e92	✕

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini	1.14 KB	cbf48c25b7e1eb3c8392ff52b85d2d3f64516cb78ae77a1dc4b0bfe44892a98f	✕
\\?\C:\Program Files\Common Files\qNyuFiCwjmRo.gif	91.62 KB	090f5731a50f9045f68bd21b3e2943d16df8bcff8db893296143c317b2cfdd0f	✕
\\?\C:\Program Files\Common Files\rdr7ouGNjf0.jpg	6.91 KB	c5f76317e892a569ad35483a41c04d2ad1256c3b723ed2fcd96d05d3101a1367	✕
\\?\C:\Program Files\desktop.ini	694 bytes	027dccfa288891310eb6ff4efc3e28c245c9e2a7415d5cdba5ce81297a3ee4bb	✕
\\?\C:\Program Files\Internet Explorer\SIGNUP\install.ins	972 bytes	8ea226bab477222593b8410d30267d5e477c76c5f257b40ab28ec6624e26b9d4	✕
\\?\C:\Program Files\Microsoft Office 15\ClientX64\IntegratedOffice.exe	1068.13 KB	cdb1623c9c689279b074df04b6a2b4d5d88ada13c67fadc6ca511102519c8110	✕
\\?\C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe	1068.13 KB	5c59f63c0bdb9a464cecabab281e3dfd289d13b7529db64019fdcf249ec407f2	✕
\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets	5.12 KB	00f4fdb82115be6d92f449f83a96e6492d0253f1f58b51d8c54cdc28fe9375bd	✕
\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets	5.57 KB	286fc4ecc6ff7928959b1d5c132ce27ff1c1d6b74531631a812351b48df15517	✕
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	7.46 KB	92398f48abb67a1250ed537240cdf83518e44e7d097a4cd526b6b42207933e82	✕
\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml	3.03 KB	84bce1a69b7b0c5c824ce5407fe9c32e8c039b3c436737515b960cf826b4ebfa	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	2.00 KB	5143ddedec8bf2763d480d6aa10e7841c65db0792b64216a19668c05bf51f459	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml	5.43 KB	04756bb82ebb1ee955d723554377934fdf7d6474e47295befcc734cf5704dff2	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1	8.12 KB	a8915e9bde5a86329514b3aa75703dfc90d012e92bcc42e2810f4f3e8d911d5d	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	17.96 KB	39b6f614b86479886080249f9df69f520438357fd24190d4404e0e88ebb88291	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	23.20 KB	79381abc672e4c682bb3465037072e69038865b93980e016e8ee01710bbf67ef	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1	78.38 KB	1a9243ec07495dc633521bb02b9adfe34c7387d889aeebe013d4e1d429ab8021	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	81.46 KB	71a0d84035bbda991a774caaffd8975a4ae8c8390836609fca3302b540316281	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	467.20 KB	099487f30c2c03878df3bc2e8c31854bfe7c049d610dfa9e29a8104a7307e910	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	1.23 KB	27ae8565ca30d18d7f40c3553d21cc4fd0347e5f191409c5562bfd68141b8152	✕
\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1	700 bytes	dc63da7505d0dfdb6fb47f213d74fd72bc88f39e0f87e0c4c6ae53defffc07fb	✕
\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	16.12 KB	4d2d55be07c911e392c22f3aeeef7254896a594626b474c107fdc14906ab4cef	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\LICLUA.EXE	317.21 KB	d6e4bba243c2427ea6d98b2b22994f6cd9af1c478397dbd13fe850f8c9def8bc	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE	200.08 KB	b8d99b0ec020912991ecd8161e2e49deb0f5a20e7d8afb7d767ab0369f6869bd	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Stationery\Desktop.ini	1.14 KB	1452188860dabde88c27d498f636c16e1f6dfc866a738855c89d76894eb761c7	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	577.19 KB	0868254694ce1d5af6efb949035d3825bcc5a3659b7a33afd73f9a332402b17e	✕

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store	9.94 KB	c49348b6ae1343bab568735578ce9be41a6c79ac1f3dcf9fefa2899eefe1daff	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat	89.45 KB	40ba05e55bb25603bf2a77f2a24a54b0bc6b6579b144a1675a839974218e9e2b	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store	127.95 KB	d81718d69c58b694e5fa48fccdf83c070568ca592caca57e6890cf47b04ee4e8	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd	655 bytes	3dd538e930bacc9d35a56ad6e5b8a5b725baeed33fcab1869177856cbf81e43a	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb	16.66 KB	f6257315b676ef38a7231ebeaec11f55228420f1d9564b57a61e5b12943b899f	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb	21.65 KB	563ae17d4cdaa5de66f0263eb7fe76ca3e734681310dd0beacb3c6d8b1d463dd	✕
\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\10.0\VSTOInstaller.exe	81.23 KB	63a8de753a1742a2a09273be3edb7bcddde7adbddff3a2b99d5eb8dc3532f29e	✕
\\?\C:\Program Files (x86)\desktop.ini	694 bytes	fe08629f4a0a9f2679e4dcecf1b083bd9e16ff34c4f73fb72d872c9b5a21bdec	✕
\\?\C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins	972 bytes	6b6c6a2176b13609ef5ba2fc934ce3953cf94bf34cd95b325656a28b9d586a8b	✕
\\?\C:\Program Files (x86)\Microsoft Office\AppXManifest.xml	4818.52 KB	e3e40c5d7e493d715eec4dd794b98abc1ff48c060b1ab934d59851bd2b378d2e	✕
\\?\C:\Program Files (x86)\Microsoft Office\FileSystemMetadata.xml	801 bytes	b05253cc23f62e652f906fc7bd1e30705a826bccedaa7839f4842118acb8147c	✕
\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM	170.95 KB	a75a9043b205a5b0be4a0e3db45e995361bae233eae4283e540443035db96b04	✕
\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS	92.76 KB	5248fa01853a5cebe8a8d5f5766a6ecc04e49e48a90ab93ff56a565bcfecd68b	✕
\\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML	35.99 KB	2eaecebb27c49257713a77a5b4dda1282b38898621c01dc4464a18b06c04dec0	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	315.08 KB	1b048682ce4ea8036cd200aeb57072d332fc6e9ada4e9d7b08dc4ed8069643ce	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	2.00 KB	074a93a31c56479f7edc5b0ec225dc0014425525a5e645fe221b471e67b72f2e	✕
\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPPREARM.EXE	23.07 KB	7f0b9398d2a8f7ffb6074e8b4ca748b47251e167532e3a2293907eeec2a77a69	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	758.40 KB	7e7271f4f05d218bfb4796859cbecfd295c1c1eb69d9e3bbad27d2684f7479de	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml	1.74 KB	f7e54406fe5fde72976f4999812954dbd7494c451e075e005315420e3b1d13cf	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml	453.61 KB	ea1b95d19cff7feacb0294aa2a5fb3dc5e10d8a38d9e31014f0c1cffcc9aef32	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml	1.74 KB	b9c58e7ac7645f2d0160b893b0e31a202667ec49c34a4a2b5a7e45e85085fbd9	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml	248.27 KB	c299f3cd2ffc471c6beb1482521a698bb40658dee31ded50e7c1616f94592000	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml	1.74 KB	cb795e158226de171a1faa5d5cdbba60c673e2fd4ebcfb29303af8a39ebd9c72	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml	1099.08 KB	cd3337d75a6804aacb5cd9b0b846681e2bc698725a1604ecbe6f2bc784eb985d	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	19.50 KB	3407c2a45add5d9cce94e8659f0054a5697b01dbf2c22ed209a1a3f069b21e1a	✕

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml	721.10 KB	7ab1d2279051db8efb91ca70f30b79dc7dd4dfd175bac7d2ac8164af9f4ff6cb	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml	1.74 KB	dcb1713b41d0135ff8523d9fbb3ef38c54fb1f5d999256a7557adf73dcbe1005	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml	1.74 KB	e62120dc99ab8d7d6b8fafd8070062f87310962e9acda0d12e8054f34814261a	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml	2.60 KB	b2b5afb0b612742eaa8b8ace36794e2dbe7b35dd7925b179b07eefad32d881e3	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	2.60 KB	589a2a11c4e0248c40b2f0f58c4d66b8edd220845bbeebd4f012d5c9ad552d71	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml	34.39 KB	32072c7f88b65f4991a19cee1751f442096aa87f3bc15051c207133f8a4a854f	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml	1.74 KB	78d1eb3dc7899edf4f5d95bf9904ac83c2f2ec0e6571430d23655691ad91aed5	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	1.74 KB	ec456046fde519acd20dcfe7388ecf372eb5797d47362a2610d999486169d620	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml	14.73 KB	d281935c304027f4dc76eefcd1b264a34089dead121389f8bd11b03ed5e5bb77	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml	349.45 KB	d59397d15a4cd65ac34c691a8790e52f11109a8fe5f371ebc5d5ed06156ca9fa	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml	1.74 KB	d745103ddb14eb542eb30d75afb5e95d096bbc80dccc1ddc4b87323bf4bb69a8	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml	55.17 KB	ed3ff058feaecaf74457aec0e57756407c44dbb9ff9fd8e3dd3756b5dedc3aaa	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml	1.74 KB	952a4d6c417ffc81177687cd7057712fb19ac2726fdcde1107f00317fd79d939	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml	9.51 KB	3ea62ce568cbe03af6c8a4e655f87e3938f93ea58d6a067878686551f60d7c9c	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml	1.74 KB	c2c0e0b26048ff475741f62c7cc727b2e2d4a88c08423f6f9d73aa4d295738ef	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml	1.92 KB	7bda326171936dbc5f355c44fcd3db6240f8a6d746ce0f5cf8040bb25a673737	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml	1.74 KB	d3f566352dbd41283f5c6ff9fb3927f656bf30d85b02d633e69c27b680b47a4a	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	4.17 KB	cc07ba492e68b9c69b22faad4169bc5e59cbc5cc220e0169c06aa27de0d7a284	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml	1.74 KB	11e11ad692eed4ab0b912f7f68c650553e7f398e91eeaaad4598c64b86c555e2	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	1.74 KB	72f6f2833a9bbb0ff0d26d0b8f95168dac67383d8b070d40f0ad7bc2d896d0f9	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml	1.74 KB	80854bf1f8b63e3dbcad1fd83c15ce66c034ace3b1c3749655eaf88d58772e5e	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml	1.74 KB	e3c4e23349ceb397572454ff6e0f3d82e4647a0cfb76c16aaa0165b3c6c28572	✕

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	1.74 KB	41c78b90e9f678309bb0618f5ea0629fda275dab12fe98361a0243e548af0db8	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	3.80 KB	1c2ac97ed3719a3151fbcf84566383bdb8ebc62ed0eeea82e40a1996dbdca54e	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml	1951.49 KB	1fc76645719ec1ec1e260b2e88f478982250eb95802d6c110903d75545f7d96a	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml	516.79 KB	665eddeb586d061cc397b1f10f8f55c93dd054e94fdcc7e3cdd96879b5d93a59	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml	10.11 KB	ff8031e9e1c77df46c7eb1874f9d32c8a60b3d87e36c6507693bd878cfa15344	✕
\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml	893 bytes	80ded59aa20e71c0f32cafce2b81a5f93e80a4e951a9f004685b90c803432637	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate64.exe	249.72 KB	2d973d179733ed58ca29168a3b56c7e53538a976c670c0e32cccca5518c924ae	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate32.exe	211.22 KB	4c0a296499dc993dd2450e49ad62261eb0ecf100c3f5d17e28c830b9017224fe	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVLP.exe	362.55 KB	d3a58e49860d2ddd6d855047f5aa934a7ae5033a839ba34f61b33c13536d083f	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF	9.32 KB	a0cd7d212a1518536e757f72a0915a92d34e51d8052302892a203c09c1526d41	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	7.04 KB	f331e786b404dff9a8142069e34677add3f322087fa625e9f3983960dbc8f9a3	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF	15.03 KB	ab7024a50115b161405e3d9a60ff580255e0adabe5dec9f68b081359a3f265af	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	7.55 KB	73bdff1279fd629a6e9ac6f8b18563536fa6d3de97f32a4b7c580286ca137288	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF	8.42 KB	30adaa8809bcdefcaf470cdbd40fe2a493fccd8876668c8fe726915ea402bc51	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF	3.68 KB	cd5baef270a87b6bf463d34a71235df5d0b5fffbdf9cc2f200f2b10f0643b8d5	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF	12.12 KB	9d75559a4c86354669fa4cf07a60e7cd03830b766cff6f1ff3e40d654a039d07	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF	1.01 KB	8dbe319369fbfad7a8cee58f285296db1cfcebb658c38cc993f1b181a717e4ba	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF	1022 bytes	3b8e134ac6c8976cf8fd21676406adb5ea82c17e7085cd1526ec27649af11c92	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	12.91 KB	a59514d7c341543d080e4209d68a708b195b0653cbaeb46c1ee8a47b0a4da174	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF	8.01 KB	c17eeb14fedded7569f301e0aafb7f2d1fe00fbdb0ede6d5508ee77541838f84	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF	12.70 KB	d0588068109c328b2c46b2f42481289e467637a78bf8507750c0bdb01d9bccfd	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF	3.91 KB	83247fb6cc5b411b673b08f621c54e799851845c48c7cf24b28384c236663123	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	5.64 KB	293bb89f33a07d3dc35871449daab95d06bd7ee64fe5e84ab00a14e93b13c013	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF	3.04 KB	188ae66fb57febf17b7889ccde961557707fc7ff3f862f470e386316cbfb4ba0	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF	10.87 KB	4cdc97d71188f707061ccabc209ef633c6d00fdaec68668e94cb288c22605ebb	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	15.46 KB	750d4a8a7ed1d03912980c5ab0425a174614fc64871a4e5888181908d46cbbf4	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF	5.70 KB	c4a7a540072e6baa4d1981701ab0e6c355f622d4eb3c509e9f2f0c9700222f03	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF	5.35 KB	dd8742b525e9e8ae2331aa2dcde29e922409a0a8215be570ed28ed3d09df514c	✕

File Name	File Size	SHA256	YARA Match
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF	5.42 KB	a26426f3a43e8f45c8dcd67c2b7895406746d58b30fe9eba5b587880d5128874	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF	1.63 KB	029b608c0a295c93389b37e4b0cb07a276837fb8006b81f571f74285a4aa04c6	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF	7.91 KB	1b2ab3413813486d6c84c336d753fb2a1018418f1af1f312c904674a3fa2e683	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF	7.33 KB	cd454876c06d8432dab2b102b98a790dcf835b70e5e4eb9a8cfc90dcf7916ef0	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF	13.45 KB	7310c26ffebb6fbdc7572295649b1c0b28b9ce79a5d9affc73e79cc27b3cf1a7	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF	8.89 KB	94942283132b016ee69334075d857f2ef0c22bc4c277c6de3537d0379fcf11b3	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF	5.29 KB	d799b5ea9687af8bf1acf201eb59d3d4968bb286f03edc8bc3577e9c7ca5e547	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	5.76 KB	375fc6647c88c0724cd9e2f7dfd4f650944a5ff699a0ac4b12b4a6d94f98e033	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	9.54 KB	7d007c1de13c96571789a81a552f6b3fa9873ea7c9894e0a0c89b2dbad750c8a	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF	5.41 KB	a7d9730a9eb5217e01272a369ec52db9b7279fc02946a2f281b4a43d8db6720a	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF	4.79 KB	03e4b2f91a2359fa2fd840402bd70df264c08af5f03f51085fc967dd5d992887	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF	4.38 KB	8d1e5075f655d910f3250c09b6478bac9d17493b250ba1438b2b246061fca56b	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF	3.81 KB	ec7702e49d6f664872830c6077221afec3d7ede07ad54c43b6ebbefd1817bf34	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF	3.55 KB	1d7a92fa719349e5d67f01bc90345b01f8d1894b1788951a59294d6cdd27f642	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF	3.46 KB	e9f32c36360e753e314c5fff296aacac6658fffe3c9a61b965f81a1fb7f1bc98	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	6.06 KB	f7e68e201d46bb2c26d174334546df3c96fb07fe23b37b905e7690bd70720d08	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	5.13 KB	c655d8ac5d8e39a540f210044782970ec08f9fd596c8b1d8579d1d0f658c1915	✕
\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\BD00141_.WMF.$$$	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✕

Host Behavior

Type	Count
Module	255
System	377
File	8991
Environment	1
-	12
Process	126

Process #2: vssadmin.exe

ID	2
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin delete shadows /all /quiet
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113314, Reason: Child Process
Unmonitor End Time	End Time: 155603, Reason: Terminated
Monitor duration	42.29s
Return Code	2
PID	1180
Parent PID	1908
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9	C:\Users\RDhJ0CNFevzX\Desktop\d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe	Sample File	204.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
63966283db8fd46ddfd282ee59dc6a52e491ccad38662731623f7aeb0df0ca54	\\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini, \\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini.$$$	Modified File	649 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1374a958c89c16b852c357bf37a8168e830a355f26198f2003400c612b8cdff3	\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini, \\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.$$$	Modified File	649 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6e748a93fcb3fcb11db0dafc3a2b47e3a00965ef65d5027687648eecdd884fd2	\\?\C:\Boot\BCD.LOG1.$$$, \\?\C:\Boot\BCD.LOG1	Modified File	520 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
fc79424cb7ae039530b4452ca34f387828abe31a7701be1a8ef15e4dc96ff7c3	\\?\C:\Boot\BCD.LOG2, \\?\C:\Boot\BCD.LOG2.$$$	Modified File	520 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
8a8d9ea8b99d55a8e9adca68344ca824a82a6ee2151214b18718ea5d25e7dcdb	\\?\C:\Boot\BOOTSTAT.DAT.$$$, \\?\C:\Boot\BOOTSTAT.DAT	Modified File	64.51 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
47662e6faa3e6ffa90c90ee916863fe848b4053b25c7f196aa7667d7b578438a	\\?\C:\BOOTNXT, \\?\C:\BOOTNXT.$$$	Modified File	521 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
63703222a5b725355360c01c4b6f76d81a4e8736201b0f8bac8b3bde0c40bddc	\\?\C:\Program Files\Common Files\1iz126n_fyjFdzvpl4k_.jpg, \\?\C:\Program Files\Common Files\1iz126n_fyjFdzvpl4k_.jpg.$$$	Modified File	55.11 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d3110d540fe7516a62049c7e2a4983885b35db04db65768b522538a1200f8afa	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\appvcleaner.exe, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\appvcleaner.exe.$$$	Modified File	2007.22 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0552f835f097eaf565525870ecf769cffba9c9d20ccc1ba9c6e22652eeea37c4	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\AppVShNotify.exe	Modified File	258.22 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0aa1281c57501690bdc25033c15380682af6c982652d2c65b52a979a4d8e7b0b	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\C2RHeartbeatConfig.xml.$$$	Modified File	4.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3efa9efec5533209917390ebaeb68afa697616e7e69f75db1a615ddd5674c2ba	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i640.hash	Modified File	622 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
00a73fe811f8097e5894edb82bcf91b3c9b9b6d3f5d4e0cbcf9e197d534c47cd	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\i641033.hash	Modified File	622 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7f81a171cc707baf489992f32446cb6ca2a71f2476dd680f9728792ef7f155e3	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\IntegratedOffice.exe, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\IntegratedOffice.exe.$$$	Modified File	1068.13 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2561c07008955e58b0b6127894f3237b7ca13cf41fa3f3fc2641135b1a1ed011	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe.$$$	Modified File	350.72 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
62ac6062d10753cc587558d1539e0bb06b982e6086cfe84b701864ec941b9dfb	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe	Modified File	5828.61 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
600a51b61867ffb565bfd4ec0b1e7fb340dfdb616ede4e87d11301a0a1bebad8	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeUpdateSchedule.xml	Modified File	5.18 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
24ef368426ce551f33078f9a21958e57e1745d0b64f44574702b65a67d889e92	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml.$$$, \\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\ServiceWatcherSchedule.xml	Modified File	4.85 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cbf48c25b7e1eb3c8392ff52b85d2d3f64516cb78ae77a1dc4b0bfe44892a98f	\\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini, \\?\C:\Program Files\Common Files\microsoft shared\Stationery\Desktop.ini.$$$	Modified File	1.14 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
090f5731a50f9045f68bd21b3e2943d16df8bcff8db893296143c317b2cfdd0f	\\?\C:\Program Files\Common Files\qNyuFiCwjmRo.gif, \\?\C:\Program Files\Common Files\qNyuFiCwjmRo.gif.$$$	Modified File	91.62 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c5f76317e892a569ad35483a41c04d2ad1256c3b723ed2fcd96d05d3101a1367	\\?\C:\Program Files\Common Files\rdr7ouGNjf0.jpg, \\?\C:\Program Files\Common Files\rdr7ouGNjf0.jpg.$$$	Modified File	6.91 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
027dccfa288891310eb6ff4efc3e28c245c9e2a7415d5cdba5ce81297a3ee4bb	\\?\C:\Program Files\desktop.ini, \\?\C:\Program Files\desktop.ini.$$$	Modified File	694 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
8ea226bab477222593b8410d30267d5e477c76c5f257b40ab28ec6624e26b9d4	\\?\C:\Program Files\Internet Explorer\SIGNUP\install.ins.$$$, \\?\C:\Program Files\Internet Explorer\SIGNUP\install.ins	Modified File	972 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cdb1623c9c689279b074df04b6a2b4d5d88ada13c67fadc6ca511102519c8110	\\?\C:\Program Files\Microsoft Office 15\ClientX64\IntegratedOffice.exe.$$$, \\?\C:\Program Files\Microsoft Office 15\ClientX64\IntegratedOffice.exe	Modified File	1068.13 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
5c59f63c0bdb9a464cecabab281e3dfd289d13b7529db64019fdcf249ec407f2	\\?\C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe, \\?\C:\Program Files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe.$$$	Modified File	1068.13 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
00f4fdb82115be6d92f449f83a96e6492d0253f1f58b51d8c54cdc28fe9375bd	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets, \\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets.$$$	Modified File	5.12 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
286fc4ecc6ff7928959b1d5c132ce27ff1c1d6b74531631a812351b48df15517	\\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets, \\?\C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets.$$$	Modified File	5.57 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
92398f48abb67a1250ed537240cdf83518e44e7d097a4cd526b6b42207933e82	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml.$$$, \\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	Modified File	7.46 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
84bce1a69b7b0c5c824ce5407fe9c32e8c039b3c436737515b960cf826b4ebfa	\\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml, \\?\C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml.$$$	Modified File	3.03 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
5143ddedec8bf2763d480d6aa10e7841c65db0792b64216a19668c05bf51f459	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.$$$, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Modified File	2.00 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
04756bb82ebb1ee955d723554377934fdf7d6474e47295befcc734cf5704dff2	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml.$$$	Modified File	5.43 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a8915e9bde5a86329514b3aa75703dfc90d012e92bcc42e2810f4f3e8d911d5d	\\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1, \\?\C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1.$$$	Modified File	8.12 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
39b6f614b86479886080249f9df69f520438357fd24190d4404e0e88ebb88291	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml.$$$	Modified File	17.96 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
79381abc672e4c682bb3465037072e69038865b93980e016e8ee01710bbf67ef	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.$$$	Modified File	23.20 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1a9243ec07495dc633521bb02b9adfe34c7387d889aeebe013d4e1d429ab8021	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1.$$$	Modified File	78.38 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
71a0d84035bbda991a774caaffd8975a4ae8c8390836609fca3302b540316281	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1.$$$	Modified File	81.46 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
099487f30c2c03878df3bc2e8c31854bfe7c049d610dfa9e29a8104a7307e910	\\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1, \\?\C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1.$$$	Modified File	467.20 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
27ae8565ca30d18d7f40c3553d21cc4fd0347e5f191409c5562bfd68141b8152	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1.$$$, \\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psd1	Modified File	1.23 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
dc63da7505d0dfdb6fb47f213d74fd72bc88f39e0f87e0c4c6ae53defffc07fb	\\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1.$$$, \\?\C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.1\PSReadline.psm1	Modified File	700 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4d2d55be07c911e392c22f3aeeef7254896a594626b474c107fdc14906ab4cef	\\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB, \\?\C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB.$$$	Modified File	16.12 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d6e4bba243c2427ea6d98b2b22994f6cd9af1c478397dbd13fe850f8c9def8bc	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\LICLUA.EXE.$$$, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\LICLUA.EXE	Modified File	317.21 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b8d99b0ec020912991ecd8161e2e49deb0f5a20e7d8afb7d767ab0369f6869bd	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE.$$$	Modified File	200.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1452188860dabde88c27d498f636c16e1f6dfc866a738855c89d76894eb761c7	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Stationery\Desktop.ini, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\Stationery\Desktop.ini.$$$	Modified File	1.14 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0868254694ce1d5af6efb949035d3825bcc5a3659b7a33afd73f9a332402b17e	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms.$$$, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	Modified File	577.19 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c49348b6ae1343bab568735578ce9be41a6c79ac1f3dcf9fefa2899eefe1daff	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\AppInfoDocument\AddIns.store.$$$	Modified File	9.94 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
40ba05e55bb25603bf2a77f2a24a54b0bc6b6579b144a1675a839974218e9e2b	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\VSTOFiles.cat.$$$	Modified File	89.45 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d81718d69c58b694e5fa48fccdf83c070568ca592caca57e6890cf47b04ee4e8	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store.$$$, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTA\Pipeline.v10.0\PipelineSegments.store	Modified File	127.95 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3dd538e930bacc9d35a56ad6e5b8a5b725baeed33fcab1869177856cbf81e43a	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd.$$$, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\ActionsPane3.xsd	Modified File	655 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f6257315b676ef38a7231ebeaec11f55228420f1d9564b57a61e5b12943b899f	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee100.tlb.$$$	Modified File	16.66 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
563ae17d4cdaa5de66f0263eb7fe76ca3e734681310dd0beacb3c6d8b1d463dd	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\vstoee90.tlb.$$$	Modified File	21.65 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
63a8de753a1742a2a09273be3edb7bcddde7adbddff3a2b99d5eb8dc3532f29e	\\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\10.0\VSTOInstaller.exe.$$$, \\?\C:\Program Files (x86)\Common Files\Microsoft Shared\VSTO\10.0\VSTOInstaller.exe	Modified File	81.23 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
fe08629f4a0a9f2679e4dcecf1b083bd9e16ff34c4f73fb72d872c9b5a21bdec	\\?\C:\Program Files (x86)\desktop.ini, \\?\C:\Program Files (x86)\desktop.ini.$$$	Modified File	694 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6b6c6a2176b13609ef5ba2fc934ce3953cf94bf34cd95b325656a28b9d586a8b	\\?\C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins.$$$, \\?\C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins	Modified File	972 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e3e40c5d7e493d715eec4dd794b98abc1ff48c060b1ab934d59851bd2b378d2e	\\?\C:\Program Files (x86)\Microsoft Office\AppXManifest.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\AppXManifest.xml	Modified File	4818.52 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b05253cc23f62e652f906fc7bd1e30705a826bccedaa7839f4842118acb8147c	\\?\C:\Program Files (x86)\Microsoft Office\FileSystemMetadata.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\FileSystemMetadata.xml	Modified File	801 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a75a9043b205a5b0be4a0e3db45e995361bae233eae4283e540443035db96b04	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM, \\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM.$$$	Modified File	170.95 KB	application/x-dosexec	Access, Write, Create, Delete, Read	CLEAN
5248fa01853a5cebe8a8d5f5766a6ecc04e49e48a90ab93ff56a565bcfecd68b	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS, \\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS.$$$	Modified File	92.76 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
2eaecebb27c49257713a77a5b4dda1282b38898621c01dc4464a18b06c04dec0	\\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML, \\?\C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML.$$$	Modified File	35.99 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1b048682ce4ea8036cd200aeb57072d332fc6e9ada4e9d7b08dc4ed8069643ce	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	Modified File	315.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
074a93a31c56479f7edc5b0ec225dc0014425525a5e645fe221b471e67b72f2e	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	Modified File	2.00 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7f0b9398d2a8f7ffb6074e8b4ca748b47251e167532e3a2293907eeec2a77a69	\\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPPREARM.EXE, \\?\C:\Program Files (x86)\Microsoft Office\Office16\OSPPREARM.EXE.$$$	Modified File	23.07 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7e7271f4f05d218bfb4796859cbecfd295c1c1eb69d9e3bbad27d2684f7479de	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	Modified File	758.40 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f7e54406fe5fde72976f4999812954dbd7494c451e075e005315420e3b1d13cf	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ea1b95d19cff7feacb0294aa2a5fb3dc5e10d8a38d9e31014f0c1cffcc9aef32	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000-0000000FF1CE.xml.$$$	Modified File	453.61 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b9c58e7ac7645f2d0160b893b0e31a202667ec49c34a4a2b5a7e45e85085fbd9	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c299f3cd2ffc471c6beb1482521a698bb40658dee31ded50e7c1616f94592000	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000-0000000FF1CE.xml	Modified File	248.27 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cb795e158226de171a1faa5d5cdbba60c673e2fd4ebcfb29303af8a39ebd9c72	\\?\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.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cd3337d75a6804aacb5cd9b0b846681e2bc698725a1604ecbe6f2bc784eb985d	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml	Modified File	1099.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3407c2a45add5d9cce94e8659f0054a5697b01dbf2c22ed209a1a3f069b21e1a	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	Modified File	19.50 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7ab1d2279051db8efb91ca70f30b79dc7dd4dfd175bac7d2ac8164af9f4ff6cb	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml.$$$	Modified File	721.10 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
dcb1713b41d0135ff8523d9fbb3ef38c54fb1f5d999256a7557adf73dcbe1005	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/x-dosexec	Access, Write, Create, Delete, Read	CLEAN
e62120dc99ab8d7d6b8fafd8070062f87310962e9acda0d12e8054f34814261a	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b2b5afb0b612742eaa8b8ace36794e2dbe7b35dd7925b179b07eefad32d881e3	\\?\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.$$$	Modified File	2.60 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
589a2a11c4e0248c40b2f0f58c4d66b8edd220845bbeebd4f012d5c9ad552d71	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	Modified File	2.60 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
32072c7f88b65f4991a19cee1751f442096aa87f3bc15051c207133f8a4a854f	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml	Modified File	34.39 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
78d1eb3dc7899edf4f5d95bf9904ac83c2f2ec0e6571430d23655691ad91aed5	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ec456046fde519acd20dcfe7388ecf372eb5797d47362a2610d999486169d620	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d281935c304027f4dc76eefcd1b264a34089dead121389f8bd11b03ed5e5bb77	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml	Modified File	14.73 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d59397d15a4cd65ac34c691a8790e52f11109a8fe5f371ebc5d5ed06156ca9fa	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml	Modified File	349.45 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d745103ddb14eb542eb30d75afb5e95d096bbc80dccc1ddc4b87323bf4bb69a8	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ed3ff058feaecaf74457aec0e57756407c44dbb9ff9fd8e3dd3756b5dedc3aaa	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml	Modified File	55.17 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
952a4d6c417ffc81177687cd7057712fb19ac2726fdcde1107f00317fd79d939	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3ea62ce568cbe03af6c8a4e655f87e3938f93ea58d6a067878686551f60d7c9c	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml	Modified File	9.51 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c2c0e0b26048ff475741f62c7cc727b2e2d4a88c08423f6f9d73aa4d295738ef	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7bda326171936dbc5f355c44fcd3db6240f8a6d746ce0f5cf8040bb25a673737	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml	Modified File	1.92 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d3f566352dbd41283f5c6ff9fb3927f656bf30d85b02d633e69c27b680b47a4a	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cc07ba492e68b9c69b22faad4169bc5e59cbc5cc220e0169c06aa27de0d7a284	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	Modified File	4.17 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
11e11ad692eed4ab0b912f7f68c650553e7f398e91eeaaad4598c64b86c555e2	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
72f6f2833a9bbb0ff0d26d0b8f95168dac67383d8b070d40f0ad7bc2d896d0f9	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
80854bf1f8b63e3dbcad1fd83c15ce66c034ace3b1c3749655eaf88d58772e5e	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e3c4e23349ceb397572454ff6e0f3d82e4647a0cfb76c16aaa0165b3c6c28572	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml.$$$	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
41c78b90e9f678309bb0618f5ea0629fda275dab12fe98361a0243e548af0db8	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	Modified File	1.74 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1c2ac97ed3719a3151fbcf84566383bdb8ebc62ed0eeea82e40a1996dbdca54e	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	Modified File	3.80 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1fc76645719ec1ec1e260b2e88f478982250eb95802d6c110903d75545f7d96a	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml.$$$	Modified File	1951.49 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
665eddeb586d061cc397b1f10f8f55c93dd054e94fdcc7e3cdd96879b5d93a59	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml.$$$, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml	Modified File	516.79 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ff8031e9e1c77df46c7eb1874f9d32c8a60b3d87e36c6507693bd878cfa15344	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml.$$$	Modified File	10.11 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
80ded59aa20e71c0f32cafce2b81a5f93e80a4e951a9f004685b90c803432637	\\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml, \\?\C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml.$$$	Modified File	893 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
2d973d179733ed58ca29168a3b56c7e53538a976c670c0e32cccca5518c924ae	\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate64.exe.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate64.exe	Modified File	249.72 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4c0a296499dc993dd2450e49ad62261eb0ecf100c3f5d17e28c830b9017224fe	\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate32.exe, \\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVDllSurrogate32.exe.$$$	Modified File	211.22 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d3a58e49860d2ddd6d855047f5aa934a7ae5033a839ba34f61b33c13536d083f	\\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVLP.exe, \\?\C:\Program Files (x86)\Microsoft Office\root\client\AppVLP.exe.$$$	Modified File	362.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a0cd7d212a1518536e757f72a0915a92d34e51d8052302892a203c09c1526d41	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF.$$$	Modified File	9.32 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f331e786b404dff9a8142069e34677add3f322087fa625e9f3983960dbc8f9a3	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	Modified File	7.04 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ab7024a50115b161405e3d9a60ff580255e0adabe5dec9f68b081359a3f265af	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF.$$$	Modified File	15.03 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
73bdff1279fd629a6e9ac6f8b18563536fa6d3de97f32a4b7c580286ca137288	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	Modified File	7.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
30adaa8809bcdefcaf470cdbd40fe2a493fccd8876668c8fe726915ea402bc51	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF.$$$	Modified File	8.42 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cd5baef270a87b6bf463d34a71235df5d0b5fffbdf9cc2f200f2b10f0643b8d5	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF.$$$	Modified File	3.68 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
9d75559a4c86354669fa4cf07a60e7cd03830b766cff6f1ff3e40d654a039d07	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF.$$$	Modified File	12.12 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
8dbe319369fbfad7a8cee58f285296db1cfcebb658c38cc993f1b181a717e4ba	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF	Modified File	1.01 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3b8e134ac6c8976cf8fd21676406adb5ea82c17e7085cd1526ec27649af11c92	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF.$$$	Modified File	1022 bytes	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a59514d7c341543d080e4209d68a708b195b0653cbaeb46c1ee8a47b0a4da174	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	Modified File	12.91 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c17eeb14fedded7569f301e0aafb7f2d1fe00fbdb0ede6d5508ee77541838f84	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF.$$$	Modified File	8.01 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b8b87cd32ae9c9ce941e22999810f9cd26c3231bc3a2e4fd766ee5c9ba60209d	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF	Modified File	3.57 KB	application/octet-stream	Access, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d0588068109c328b2c46b2f42481289e467637a78bf8507750c0bdb01d9bccfd	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF.$$$	Modified File	12.70 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
83247fb6cc5b411b673b08f621c54e799851845c48c7cf24b28384c236663123	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF	Modified File	3.91 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
293bb89f33a07d3dc35871449daab95d06bd7ee64fe5e84ab00a14e93b13c013	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	Modified File	5.64 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
188ae66fb57febf17b7889ccde961557707fc7ff3f862f470e386316cbfb4ba0	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF.$$$	Modified File	3.04 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
4cdc97d71188f707061ccabc209ef633c6d00fdaec68668e94cb288c22605ebb	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF.$$$	Modified File	10.87 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
750d4a8a7ed1d03912980c5ab0425a174614fc64871a4e5888181908d46cbbf4	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	Modified File	15.46 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c4a7a540072e6baa4d1981701ab0e6c355f622d4eb3c509e9f2f0c9700222f03	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF.$$$	Modified File	5.70 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
dd8742b525e9e8ae2331aa2dcde29e922409a0a8215be570ed28ed3d09df514c	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF	Modified File	5.35 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a26426f3a43e8f45c8dcd67c2b7895406746d58b30fe9eba5b587880d5128874	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF	Modified File	5.42 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
029b608c0a295c93389b37e4b0cb07a276837fb8006b81f571f74285a4aa04c6	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF.$$$	Modified File	1.63 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1b2ab3413813486d6c84c336d753fb2a1018418f1af1f312c904674a3fa2e683	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF.$$$	Modified File	7.91 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cd454876c06d8432dab2b102b98a790dcf835b70e5e4eb9a8cfc90dcf7916ef0	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF.$$$	Modified File	7.33 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7310c26ffebb6fbdc7572295649b1c0b28b9ce79a5d9affc73e79cc27b3cf1a7	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF.$$$	Modified File	13.45 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
94942283132b016ee69334075d857f2ef0c22bc4c277c6de3537d0379fcf11b3	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF.$$$	Modified File	8.89 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d799b5ea9687af8bf1acf201eb59d3d4968bb286f03edc8bc3577e9c7ca5e547	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF.$$$	Modified File	5.29 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
375fc6647c88c0724cd9e2f7dfd4f650944a5ff699a0ac4b12b4a6d94f98e033	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	Modified File	5.76 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7d007c1de13c96571789a81a552f6b3fa9873ea7c9894e0a0c89b2dbad750c8a	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	Modified File	9.54 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a7d9730a9eb5217e01272a369ec52db9b7279fc02946a2f281b4a43d8db6720a	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF	Modified File	5.41 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
03e4b2f91a2359fa2fd840402bd70df264c08af5f03f51085fc967dd5d992887	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF.$$$	Modified File	4.79 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
8d1e5075f655d910f3250c09b6478bac9d17493b250ba1438b2b246061fca56b	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF.$$$	Modified File	4.38 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ec7702e49d6f664872830c6077221afec3d7ede07ad54c43b6ebbefd1817bf34	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF.$$$	Modified File	3.81 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1d7a92fa719349e5d67f01bc90345b01f8d1894b1788951a59294d6cdd27f642	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF	Modified File	3.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e9f32c36360e753e314c5fff296aacac6658fffe3c9a61b965f81a1fb7f1bc98	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF.$$$	Modified File	3.46 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f7e68e201d46bb2c26d174334546df3c96fb07fe23b37b905e7690bd70720d08	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	Modified File	6.06 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c655d8ac5d8e39a540f210044782970ec08f9fd596c8b1d8579d1d0f658c1915	\\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF.$$$, \\?\C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	Modified File	5.13 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4713834aef2c852bbeda1b84a77d14f49877cff0020afca7f74960933e30b0a8	\\?\C:\Program Files\Common Files\microsoft shared\ClickToRun\readme.txt, \\?\C:\Program Files\WindowsPowerShell\Configuration\Sch... ...s (x86)\Common Files\Microsoft Shared\TextConv\readme.txt, \\?\C:\Program Files\Common Files\microsoft shared\ink\sk-SK\readme.txt	Dropped File	438 bytes	application/octet-stream	Access, Write, Create	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\$Recycle.Bin\.	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\..	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\.	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\..	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini	Modified File	Access, Write, Delete, Read	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\.	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\..	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini	Modified File	Access, Write, Delete, Read	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini.$$$	Modified File	Access, Write, Create	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\$Recycle.Bin\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\.	Accessed File	Access	CLEAN
\\?\C:\Boot\..	Accessed File	Access	CLEAN
\\?\C:\Boot\BCD	Accessed File	Access	CLEAN
\\?\C:\Boot\BCD.LOG	Accessed File	Access	CLEAN
\\?\C:\Boot\BCD.LOG1	Modified File	Access, Write, Delete, Read	CLEAN
\\?\C:\Boot\BCD.LOG2	Modified File	Access, Write, Delete, Read	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini.$$$	Modified File	Access, Write, Create	CLEAN
\\?\C:\Boot\bg-BG\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\bg-BG\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\BOOTSTAT.DAT	Modified File	Access, Write, Delete, Read	CLEAN
\\?\C:\Boot\BOOTSTAT.DAT.$$$	Modified File	Access, Write, Create	CLEAN
\\?\C:\Boot\cs-CZ\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\cs-CZ\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\BCD.LOG1.$$$	Modified File	Access, Write, Create	CLEAN
\\?\C:\Boot\BCD.LOG2.$$$	Modified File	Access, Write, Create	CLEAN
\\?\C:\Boot\da-DK\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\da-DK\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\da-DK\readme.txt	Dropped File	Access, Create	CLEAN
\\?\C:\Boot\de-DE\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\de-DE\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\de-DE\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\el-GR\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\el-GR\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\el-GR\readme.txt	Dropped File	Access, Create	CLEAN
\\?\C:\Boot\en-GB\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\en-GB\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\en-US\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\en-US\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\en-US\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-ES\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\es-ES\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\es-ES\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-MX\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\cs-CZ\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\es-MX\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\et-EE\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\et-EE\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\fi-FI\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\fi-FI\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\fi-FI\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\Fonts\chs_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\cht_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\jpn_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\kor_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\malgunn_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\malgun_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\meiryon_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\meiryo_boot.ttf	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\Fonts\msjhn_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\msjh_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\msyhn_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\msyh_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\segmono_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\segoen_slboot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\segoe_slboot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\wgl4_boot.ttf	Accessed File	Access	CLEAN
\\?\C:\Boot\Fonts\readme.txt	Dropped File	Access, Create	CLEAN
\\?\C:\Boot\fr-CA\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\fr-CA\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\fr-FR\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\fr-FR\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\fr-FR\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\hr-HR\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\hr-HR\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\hu-HU\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\hu-HU\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\hu-HU\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\it-IT\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\it-IT\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\it-IT\readme.txt	Dropped File	Access, Create	CLEAN
\\?\C:\Boot\ja-JP\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ja-JP\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ja-JP\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\ko-KR\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ko-KR\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ko-KR\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\lt-LT\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\lt-LT\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\lv-LV\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\lv-LV\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\memtest.exe	Accessed File	Access	CLEAN
\\?\C:\Boot\nb-NO\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\nb-NO\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\nb-NO\readme.txt	Dropped File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\nl-NL\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\nl-NL\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\nl-NL\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\pl-PL\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pl-PL\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pl-PL\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\pt-BR\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pt-BR\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pt-BR\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\pt-PT\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pt-PT\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\pt-PT\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\qps-ploc\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\qps-ploc\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\qps-ploc\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\Resources\en-US\bootres.dll.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\Resources\en-US\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\Resources\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\ro-RO\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ro-RO\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\ru-RU\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ru-RU\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\ru-RU\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\sk-SK\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sk-SK\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\sl-SI\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sl-SI\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\sr-Latn-CS\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sr-Latn-CS\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sr-Latn-CS\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\sr-Latn-RS\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sr-Latn-RS\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\sv-SE\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sv-SE\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\sv-SE\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\tr-TR\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Boot\tr-TR\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\tr-TR\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\uk-UA\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\uk-UA\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\zh-CN\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-CN\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-CN\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\zh-HK\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-HK\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-HK\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\zh-TW\bootmgr.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-TW\memtest.exe.mui	Accessed File	Access	CLEAN
\\?\C:\Boot\zh-TW\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\Boot\readme.txt	Dropped File	Access, Write, Create	CLEAN
\\?\C:\bootmgr	Accessed File	Access	CLEAN
\\?\C:\BOOTNXT	Modified File	Access, Write, Delete, Read	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d44df8fc28ccfa08c75e9965b3cc145d82111137e70b96946331e113ec6dd0b9.exe"	MALICIOUS
vssadmin.exe	vssadmin delete shadows /all /quiet	CLEAN

YARA / AV

YARA (56)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Gibberish	Gibberish 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	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

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