MALICIOUS

Classifications: Injector | Wiper | Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe**
ID	#5442858
MD5	3289319de6623ddcb71671df29e7be85
SHA1	f1586ad8edadb0593983186107b163fd3aaa05f0
SHA256	9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f
File Size	172.00 KB
Report Created	2022-09-20 09:55 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 90 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #2) cvtres.exe modifies the content of multiple user files.			
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #2) cvtres.exe deletes multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) cvtres.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 1023 files by appending the extension ".crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe modifies memory of (process #2) cvtres.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe alters context of (process #2) cvtres.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Hide Tracks	Hides files	1	-
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe hides the file "C:\Users\RDhJ0CNFevzX\Desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe" by setting its "hidden" attribute.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #2) cvtres.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) cvtres.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe starts (process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe reads from (process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-

Score	Category	Operation	Count	Classification
	• (Process #1) 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Hide Tracks	Changes folder appearance	71	-

- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessibility".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessories".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet PC".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Administrative Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Maintenance".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Microsoft Office 2016 Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\StartUp".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\System Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\All Users\Microsoft\Windows\Start Menu Places".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group1".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group2".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\AccountPictures".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Desktop".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Documents".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Downloads".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Libraries".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Music".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Pictures".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\Public\Videos".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Application Shortcuts".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Burn\Burn".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Burn\Burn1".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Burn\Burn2".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Burn\Burn3".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\History".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group1".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group2".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group3".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\AccountPictures".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Libraries".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\SendTo".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Contacts".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Desktop".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Documents".
- (Process #2) cvtres.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Downloads".

Score	Category	Operation	Count	Classification
1/5	Persistence	Installs system startup script or application	4	-

- (Process #2) cvtres.exe adds "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\StartUp\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx" to Windows startup folder.
- (Process #2) cvtres.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx" to Windows startup folder.
- (Process #2) cvtres.exe adds "C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\StartUp\IF_YOU_WANT_TO_GET_ALL_YOUR_FILES_BACK_PLEASE_READ_THIS.HTML" to Windows startup folder.
- (Process #2) cvtres.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\IF_YOU_WANT_TO_GET_ALL_YOUR_FILES_BACK_PLEASE_READ_THIS.HTML" to Windows startup folder.

1/5	System Modification	Creates an unusually large number of files	1	-

- (Process #2) cvtres.exe creates an above average number of files.

-	Trusted	Known clean file	1	-

- File "c:\users\rdhj0cnfevzx\appdata\local\microsoft\vault\userprofileroaming\latest.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx" is a known clean file.

Mitre ATT&CK Matrix

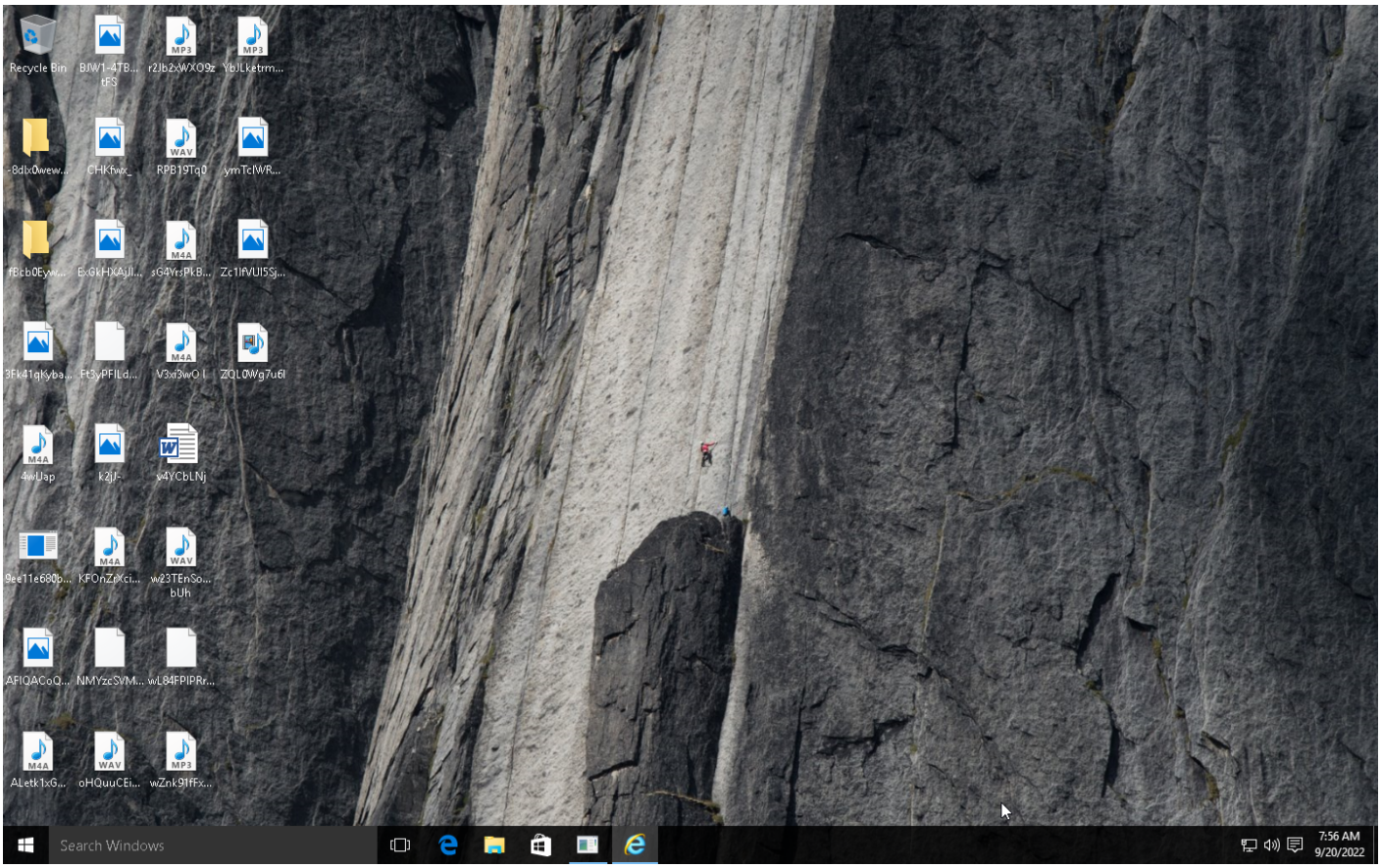
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1158 Hidden Files and Directories		#T1158 Hidden Files and Directories	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window				#T1005 Data from Local System			#T1485 Data Destruction
				#T1045 Software Packing							
				#T1036 Masquerading							

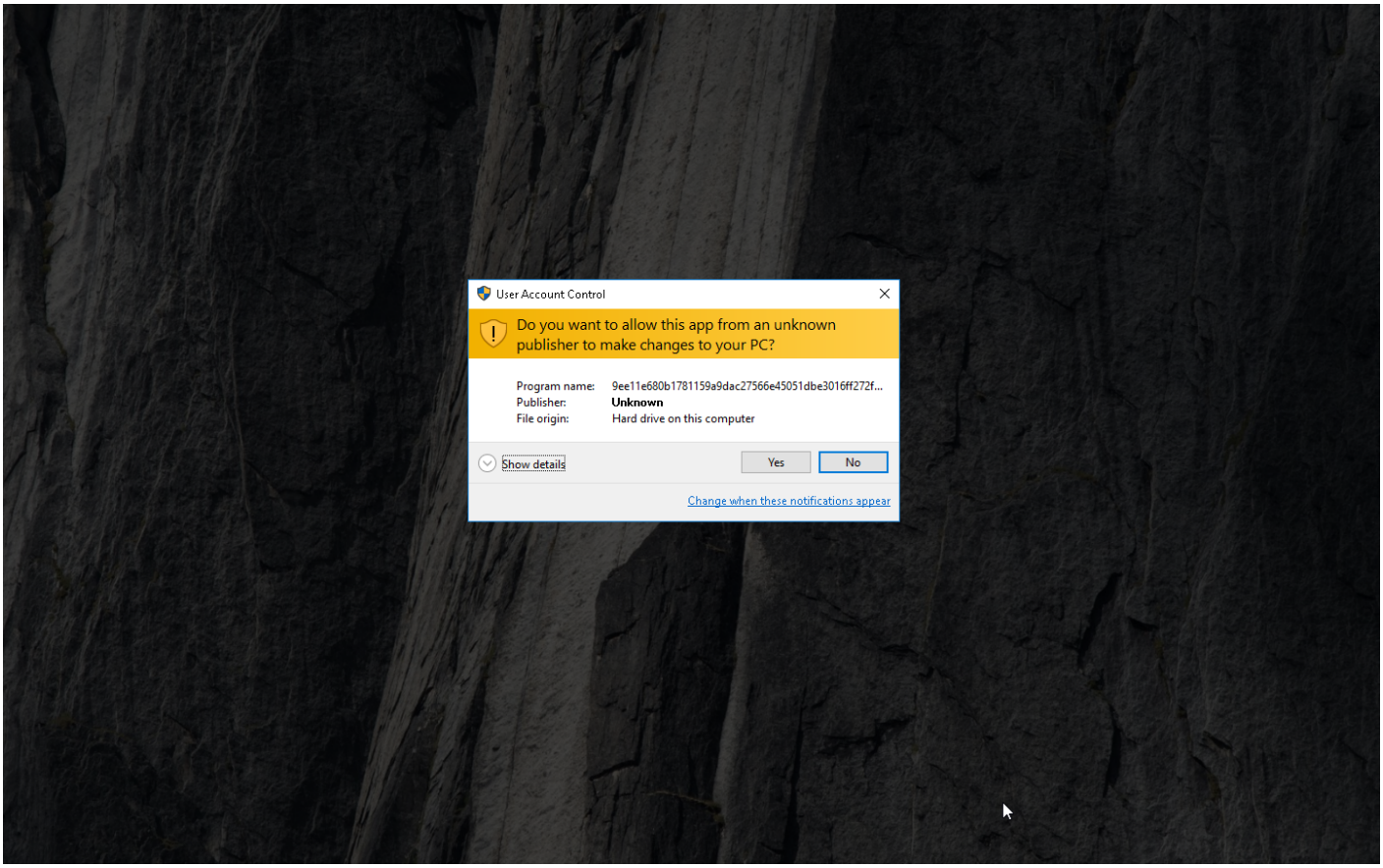
Sample Information

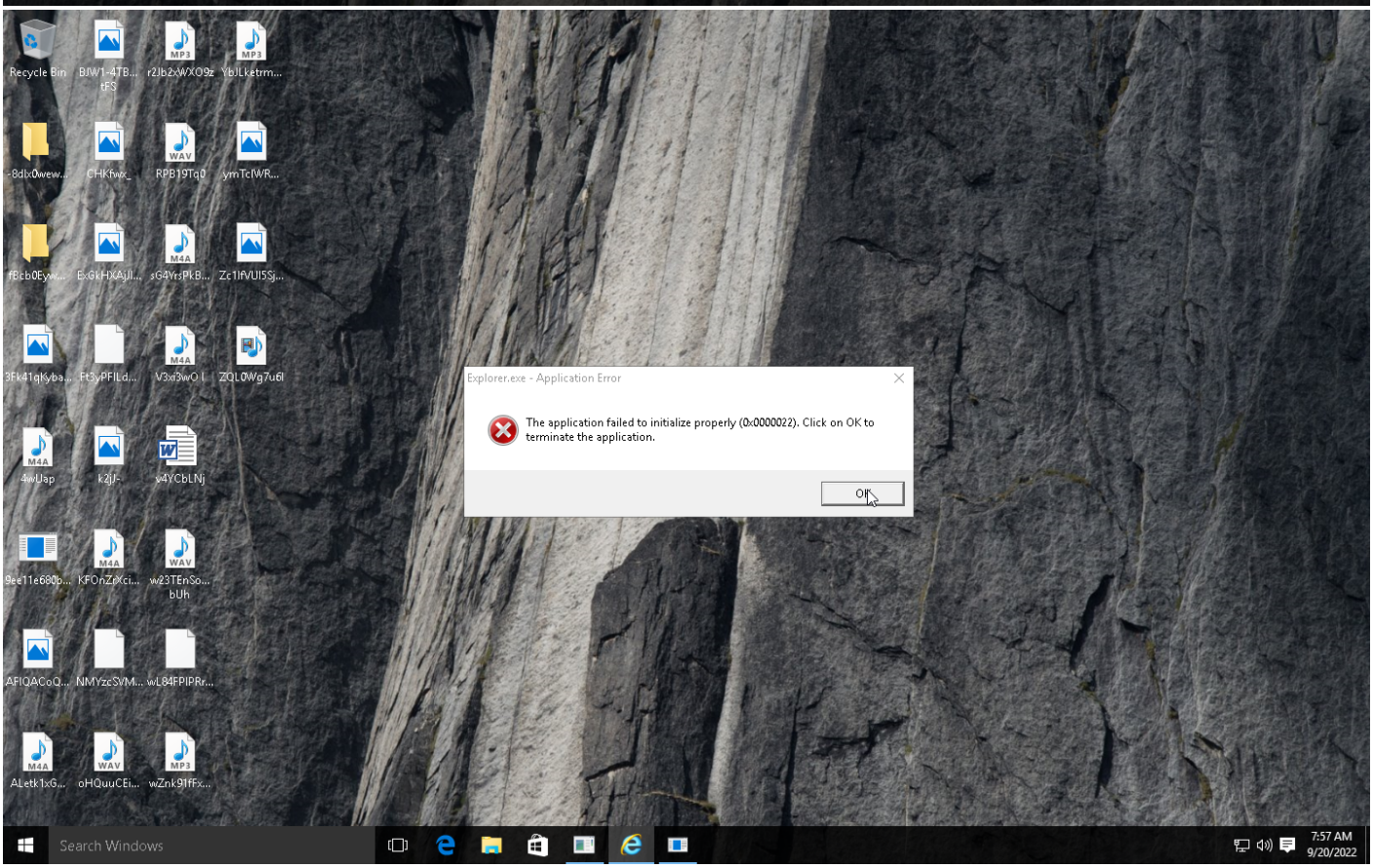
ID	#5442858
MD5	3289319de6623ddcb71671df29e7be85
SHA1	f1586ad8edadb0593983186107b163fd3aaa05f0
SHA256	9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f
SSDeep	3072:3kloOnc4jWXAzcqYUsnJXzn+uSlLJAvDd/oV/kXDMLRyRQxFltJZDpyzA2H1Sgig:0KGWXOY94eQV/W4SCF7JZDmA2H1Sp
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe
File Size	172.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-09-20 09:55 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
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	0


Recycle Bin
Search Windows
7:56 AM
9/20/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 9ee11e680b1781159a9dac27566e45051dbe3016ff272f...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

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

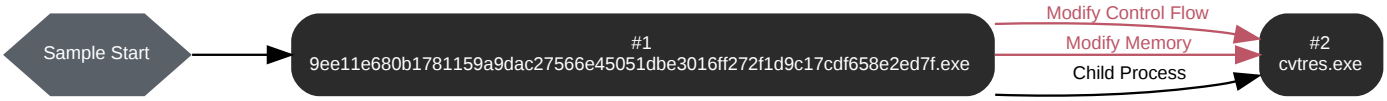
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65235, Reason: Analysis Target
Unmonitor End Time	End Time: 107576, Reason: Terminated
Monitor duration	42.34s
Return Code	0
PID	3936
Parent PID	1648
Bitness	32 Bit

Host Behavior

Type	Count
Module	35
System	17
User	1
File	4
Window	1
Process	1
-	3
-	12

Process #2: cvtres.exe

ID	2
File Name	c:\windows\microsoft.net\framework\v2.0.50727\cvtres.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103838, Reason: Child Process
Unmonitor End Time	End Time: 305262, Reason: Terminated by timeout
Monitor duration	201.42s
Return Code	Unknown
PID	3080
Parent PID	3936
Bitness	32 Bit

Injection Information (9)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x401000(4198400)	0x15000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x416000(4284416)	0x1400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x419000(4296704)	0x1200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x41c000(4308992)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x41d000(4313088)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x41e000(4317184)	0x4000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88	0x2e2008(3022856)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	0xc88 / 0xc54	0x415d8c(4283788)	-	✔	1

Dropped Files (2178)

File Name	File Size	SHA256	YARA Match
-	65.58 KB	dd8b85247f58a60c3a5e5153ea447e1ddc131c90f6969f027cfe42585256aabf	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{E347E1DF-602B-433D-B049-596C6048612B} (1) - 3128 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	300 bytes	880ccb2287431ea9c087e65357a00139a948142e991565529b72a572d77fc421	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group2\1 - run.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.08 KB	5698bc5992fd3c04de7fe8fbbdf5322ecc61770a12ccd02df81dfa782d622907	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TCPrefs_2_D3E71568CFF98B44AA768B6125CC6184.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	204 bytes	a99fd5f8151bb0a569df634bbf878ef6034ba671d96ec74fb759a9b0e1c70685	✖
-	2.15 KB	4c4fbe32af44be1ab54353fd29c569ebb74f53cb9b5f754e77b096b4d72d0fac	✖
-	2.61 KB	fdc3fa4fef644c22b3aafc45c0d5a95fee2550d072e908747b05c729e53720bb	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\8L05D5LK\favicon[1].ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	4.19 KB	5c515dce6537271ae3201088a32c06286385b2441f2f07ce17e93d3b22ed41a4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\AutoPlayLogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	4.56 KB	d10695f2975bb83a275dc9c32db753bce9cf8e6679b66a88e8199ae57141f8a7	✖
-	279 bytes	79e14823fc7b287e40c9cde214dc0568b461fdcbac15e463e44a9c66468e4c69	✖
-	1.32 KB	434ef515937a8b23637e8cbc429a6af4bb83be1c55f021853f2f8a14318abdbb	✖
-	24.62 KB	0f778442f6e1a923a7a5b5680867a5ff7e4ed1dab49cd8ddd126eb03e87179b2	✖
-	1.09 KB	1169b27e51159cf5a43864824bf6a8b8149fc2173b76b8b1f7904bf9a4c520b7	✖
-	2.02 KB	8c7f41e5b9996b3c5971690586b6140b4fa069f22664fe660a3add9c3e483ec4	✖
-	36.00 KB	5068a913cbcbea91d534589133208c5f49bf02a10adf730b495b7dcb47dd1342	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{476867b0-6c71-41f9-b8ee-957d2c806c59} (0) - 3924 - winword.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	845 bytes	0de6f0373b18c0f56efbeaf195e4fff613dc88a43f142dd46c0b7001518ec259	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\edb.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	e1dc8b5b9781389faff8509ec1b0b90c020024175ddc0be4dea2ab021c5ffbee	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\ScreenshotOptIn.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	432.01 KB	b6ffd6114748daf719e683e5157f5f693c53b3511e1eeb3a4dab4245cbde20eb	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{12E262E7-D2B6-4D7F-8C8E-099A50A4E1B9} (0) - 3576 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	837 bytes	09493d5e3c3ad9da400da9056c2d1bda1da2778397392d84499a18b40273a4ba	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{D32DDB02-A781-4D79-BBB3-90DD7781C33D} (0) - 3812 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	279 bytes	2778f34525289a8c37c1ab3b878bee091a725caf6ad5a94810a6c471695a20bb	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (1) - 3500 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	483 bytes	32cbf0c96a682b29e794e5849d27a5174b5543dab31a2c8288497af4825d30fa	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{6b789349-1698-4ea5-b0f1-2664e9e9ae46} (0) - 3248 - outlook.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	283 bytes	84d6fa8848d73d97177f111e90d4721eb087da5904239b5f91b8de83301db947	✖

File Name	File Size	SHA256	YARA Match
-	790.79 KB	290c39cec9af73ba440544968e229a190a4b48d3a9e6680f190cb4403f0a633a	✖
-	24.62 KB	749c2df00d2de4fd377ef4e12b53156af4e72fcb795319e6905201c2c75fece6	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\gamedvr\knowngamelist.bin.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	52.56 KB	75c22250be41a91bf3750d53022847de8fb7823bc41d3387309e338f73f9f546	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\caches\{3da71d5a-20cc-432f-a115-dfe92379e91f}.1.ver0x0000000000000019.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	42.64 KB	a7b553052a80804cfdbbe078b26806f66dd8a9e1546728c7d78cfe4cd91042ad	✖
-	1.07 KB	589adacd2e368fe5b8373a8804e113b9371be823877888361b2f9138262e1cff	✖
-	80 bytes	5148fd2571e37bab89101c083257c8c320e93b102a19703cb0929e6f164cc3e7	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{5abd4b01-aba3-41bd-9fd7-3db72380d196} (0) - 3620 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	279 bytes	17ded93d5a889df37a1eb181d4cbac2290440f61309c3fcb6416b0912ba4ff1d	✖
-	2.17 KB	7ce6bcdd5345c3fa8ccea25dc0ba908596d58774015f82a0f56b6bfb4032d39c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (0) - 3500 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	837 bytes	990ad4e0cd0fe3b2ac439c70fd07e5becd7fbea4ad9845203bb06f27e76076df	✖
-	8.00 KB	04033a02c5debf8905cfb8f62dc74fb96ac47cbd5091a15f6165c7826031dedf	✖
c:\users\public\music\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	380 bytes	8a9c3d0351db0261052f87ca0fc757a064ab75c08eccf099a4482f259b8172cc	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group3\07 - event viewer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1015 bytes	7c0c08efaad1dd4d49abc41defd5e4118975eb1ef0d98ef24819dfe2df91ad50	✖
-	2.05 KB	17a47251a683ad9e1a0205fe323935a4286f9a8576a18f8cded4b9e63901c0ad	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group3\09 - Mobility Center.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1015 bytes	c69929e81cfd996d2e7622f0dd8aa270887c692419548ba420e6697cd59ca43d	✖
-	2.54 KB	5d3313f0a40d350552b810ab8eadba1c8e79bf815139e47f62964e26c16c9bdf	✖
-	1.09 KB	76843caf1a2a6f20d30b6a97b395abe60c302e2e8f2eb08409de7bb3d444e2a0	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group3\01a - Windows PowerShell.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.10 KB	ad1d99f65437b3db654dd2f172291e38bbb124b3616acb7816a3946ded18531a	✖
-	1.44 KB	12c6336959a5657547cc1eb9b802444bc83955f348cee7040d248be440d4c966	✖
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	568 bytes	6b34f5d76ff3f3172e2d7cb3aebfc63a7fac773b8c433408b9cd1a944841cf0b	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install-PerUser_2021-02-11_132743_ca8-cac.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	228.16 KB	7fd8ca66fd6bd571edf16d1df8defe2e83a00a6b9492e5407136d8d0c250d41e	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WebCache\V0100006.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	512.00 KB	d9086ff50af6d4cc5aa20f04cf27440b3dc982e1a2cf7e01ecafa6d337f9ebf6	✖
-	273.95 KB	4db88b0878e0229bcd3b16c54c5d1d665fbd476b31ad3e14b573c2ceb9b621c1	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (0) - 776 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	279 bytes	6652121aa2f572510844871418e76f1a2dee8d66b76457881ce20d033043b669	✖

File Name	File Size	SHA256	YARA Match
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2txyewy\ac\appcache\c1j92j4x\2\c__windows_systemapps_microsoft.windows.cortana_cw5n1h2txyewy_cache_coobe_cortanaicon[1].png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	6.44 KB	b671338d996e3167c4010974540789c6cea877225b52d754d752d878453e1663	✖
c:\users\default\appdata\local\microsoft\windows\winx\group2\5 - task manager.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1021 bytes	a885c577a756ccc53cbb3750a8e4661b3663be6ff7bb1f3b65592bd2c990bc31	✖
-	1.13 KB	a19c7dee5d7125f4064ffd3396a688cee2ccf8effc4b5612db068b45eac9ff4b	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\setup\logs\install_2021-02-11_131858_ed0-ed4.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	61.49 KB	9e776a202f722bc6d5bc21e0e83ecc4a1abea40ebc5652f1406a9665cb922fb5	✖
-	26.38 KB	4f7918bf6f1a9803e31a17207052d651787ac65ca2d9542e7c405cd610344a41	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\27771a56.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	13.40 KB	5202b2e48f23d862cfe88822d95a06b250b7d70cc1f0124c1127ba7255e5ec22	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{76787746-0ef6-4759-84bc-631b78c93eb7} (1) - 3608 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	483 bytes	db3926687491a281808b1c49448ad8c6ce3fa24b6f9f01bbc7f209ff9ec4626c	✖
-	2.75 KB	f0721cf077200d10bedbdec08bc125dbe7b114811c1508c0e484a3420eea35be	✖
-	1.10 KB	55e31869385a48e41f801d55d738d70a97ce8d9e15dcff173accd8a1f4609769	✖
-	501 bytes	1ccdd07b99097fb5354465e2437bb13d330d89068a5b063d8f513265e453a452	✖
-	321 bytes	aaabccbe093db361eebdebc2782e64ac3cfedb4e2ebbc46925a549db7b3ddcbf	✖
c:\users\public\pictures\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	380 bytes	fb9442838dfd009ffd6702a845ef225eecfc0b5e3bbc09364c66c167b66ce094	✖
c:\users\default\appdata\local\microsoft\windows\winx\group2\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	332 bytes	5f827696267e972210e77f8a2c4e701977888d28168a4ea9210b8c23dbeaeb2b	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{6b789349-1698-4ea5-b0f1-2664e9e9ae46} (0) - 3248 - outlook.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	845 bytes	bd46a765bd1141da6c435ddfcee132a9995391b44f92f26074297ffe33f28277	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install_2021-02-11_132742_c8c-c90.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	61.49 KB	26af47bf402a2b22397015a4ebd300f143a4f348346b09f5b0b235237f372bdf	✖
-	1.15 KB	7399ec72b5418acc5941383263bf3313ae412c3da1f637e8ac0cb57c17ad3547	✖
-	1.07 KB	09ec6613c930a2dcf20d0f79de079a49577f8df4573be319557774556d6d8a15	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_2\screenshotlogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	4.57 KB	a69eb3144eeb0b328a79757b545ce81822c1495b4a6743629e3a90ba60e99843	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\autoplayoptin.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	374.24 KB	48adf118b5579fbee7495fc26f15593563779e64cf1688d82ba3e47791e5e5a2	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{C9F887AB-1565-4D03-878C-E985B67FFEF2} (0) - 3748 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	837 bytes	b4c0a32297960ac68d6e536097c88ac5ad57193e31904dc1ed2c48c9a3e0e73b	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\amd64\filesyncapi64.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	256.00 KB	68404875ff629b362c1450d010501ee6a702ad96153c549f715ff0fba32071b8	✖
-	56.95 KB	68b0b413e61e398d5218fa19e744d6137de19d86714c32df3a9673aa1d3c4925	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	82f43f835574530d9a3e0fa086fcaab795e625910f05b56e6ab454eb8da10ccd	✖
-	80 bytes	1b9278485b6e07398345bf09ae5a5de674ea8828ad20a53451682b25b1bdec4b	✖
-	1.11 KB	cd47ef02db9cc172f749290aea7613c94e030e083be604d03e9d93e4105bfbad	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\7a67116a.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.26 KB	f6db98c54e1e667137e9b6237a9d31d292a3a6fba456e025e3409530bb8fa399	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_256.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	24 bytes	3f2720cf72e3f6aa6ea624f12323767ee85aa8250403bbd63f0eaff5d6efc844	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\ad9a3041.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	9.63 KB	5889179ca119305e3ca0b8e7642491ed7ca549c016213c7a8b2e0711cc4999d1	✖
-	23.71 KB	1c88eb5a443c6ca1da71744a9e04d1cd595df17546e7fa3b6ba5319de26b481c	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\collectonedrivelogs.bat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	5.71 KB	5429c849aae1e5d4fba9b7d6d8fa2933741ab3628918a53ea7081002273c2b2c	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Microsoft.BioEnrollment_10.0.10586.0_neutral__cw5n1h2txyewy\ActivationStore\ActivationStore.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	3eacb83a8788b2f982b84ee980dc3704592c186036867462fa0d2d5a94189782	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group1\1 - Desktop.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.08 KB	f1567047c2a4e0d3c9eeadfb1dacb54523a3e1c3baa2d689cd5d3087de535bcf	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	2.18 KB	10c76e5d4ba201b6e21821aca82ec4ea523ce9f6edc09d90f4ade5ad9af743fb	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000017.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	108.52 KB	0660b35b5e76bd8e47672ba6f59f01f888a64a4df12ab79713687cbb73140fb6	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\d242e6bf.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	3.76 KB	9415ec8723d4eb0ba039de7d253b975ada536160bcc1c833a25f70e977152704	✖
-	174 bytes	cb1885f879e3c4a687d849f925f0af2f676f31d7d2b2d9681f72b436163703f2	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\WnsClientApi.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	373.69 KB	c96c6ac9382646cc0b8d4b7fbeb630c52a50e4049bb25834da9731e01347fee9	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v4.0\usagelogs\sdiagnhost.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	5.47 KB	924cbbcc1458a21ee226669035bff1e43dc88e6d6e50eef317f9f9784682a929	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{730eed67-cb03-48eb-b6a2-97fadd6a81fb} (1) - 3644 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	483 bytes	23d9dc852ebb7a4a4dd44536d93aa658baf42b12a2d8fa3aa3f3f7232b91d41e	✖
-	1.13 KB	ebd6d610da3a81064fa5a02e4f67897360d4d98726a6d64e54bff378043b381a	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{c9f887ab-1565-4d03-878c-e985b67ffef2} (0) - 3748 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	279 bytes	a28bd09fd6fd841cbe32bb4f2413852be87187de62b1751a0430f3bb1dbb5a51	✖
-	1.22 KB	4294b1341112840237944a465c1ce01c4ce5d6d7522f5311b1f6c57120949602	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	aa0f6793182693f1c5935ce40936bc0cbf8e4e35c47e9deea4411eebb634029f	✖

File Name	File Size	SHA256	YARA Match
-	4.55 KB	2d0190c56cb97dedcb945567ecdfba6a744cdb588d9e631320565dde0d1c45fb	✖
c:\users\default\appdata\local\microsoft\windows\winx\group3\08 - power options.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.05 KB	e31a854a6e7ade7e9b7deb646732319d53a22888c9501c653adee28ca68f7b15	✖
-	50.67 KB	d3a704d07e3d5e9bb7dd5bded4768aff2abdfd9b542e82501e09fc24e519c624	✖
-	1.08 KB	7fa76e5d0760b346db219545bf9338b7bf550eaa59dac77c8c94789d3f01236f	✖
-	1.21 KB	88a6735ddad1e5b5c5a24b9982192c35a23e01981c208dbd865b1c24961fce6a	✖
-	24.62 KB	45fb24d33c298625bae626d59a396bbdf3416ce20b4d99f8de74c36e2a7f0a3f	✖
-	576 bytes	9556b3501bfa33db5e3e33f700ea0336f51d99dd9d847d1c8619558eb4b45600	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\LogFiles\edb.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	512.00 KB	39651697284635c4106cdf83337f08f1c0d5286b7a78cf76bc2d3ef42b4e75df	✖
-	433 bytes	6c395c0c431a0cfdb74ecf5049feee26fda38b6179f3a5d7b4451fff20884231	✖
-	1.09 KB	96ac84ebc21a1f9d96344d59cebcab2df960eb27764a51a087bfea69800bb2c0	✖
-	25 bytes	06ff150994ab9839e3cbe38d672996055d2430bd9eed1844ec1d5b15053b9daa	✖
-	1.09 KB	49b47fa1845aa1397758b1fbddae07f9c019cb4e5caab675b6745acf7bdea590	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{d32ddb02-a781-4d79-bbb3-90dd7781c33d} (1) - 3812 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	483 bytes	efacb2bc8c3792644bbd4e77e4afbe503dfb6d918646c030ec6defdef66754ed	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (1) - 776 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	300 bytes	b927713d723501d5675db7c55dc8aed2c1d71d31513b7ce4ba6ae71a7242e027	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{5abd4b01-aba3-41bd-9fd7-3db72380d196} (1) - 3620 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	300 bytes	93566382ffb4877867811a5264163e9aa5d1ece5f0b71b9a3d09164e96708aae	✖
-	1.09 KB	f5a696c9b8ca7d8e31b50bc134a151846c7e8fb7cadc0dac0a878ed32c057fbf	✖
-	59.11 KB	c7752f8fca7285fd88d8400159cd4becd1d5c27dbc43ab04b931704d67306274	✖
-	52.16 KB	9819287e541cd37e0b07a5a055bba354095653f9b92220872db71887344633a3	✖
-	1.19 KB	fa11ceaa96b6365347e39954d732d4f1ef833c028ca41a8c6758dd828dd1e2d2	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Uninstall-PerUser_2022-08-03_151233_600-778.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	71.83 KB	2470ba7575d8189fdcf21f2ae5c45191297a85d8e3dda8b1c3b7b50f5b7c44c3	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	73e6a5abf7883180bf336661522acb637ecec3daa4038950c452900b50e0db32	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	2.18 KB	863d083bb71490e9b7ec028b449e16dd5216314b4e47613ebe43d14b75ece2d9	✖
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell ISE (x86).lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.24 KB	ac6db52f08cac4da3c4fdadc38c992a093ed8a8f03f3e742e5e860e65321787d	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\webcache\v01.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	29b8514225d66f3cad0ab6132797d2ac9a4d1bdfbe17eb35eeb612f121e5c553	✖

File Name	File Size	SHA256	YARA Match
-	72 bytes	d07a0cca26057dc9f0be31af8073f428229aaf95aa1538ab07e41c69b7d0d7b1	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.27 KB	4bd5f4a03ec6dd970f539216d8af66b118ad3d253caf99a09695b2fe791f4ed8	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (0) - 3500 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	279 bytes	bfeb06eed1776000a07912b8486eeb50569f0a739a88b1049b97be40d7828cae	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\1ced2593.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	4.57 KB	54d8197589535f2046a4f1c552e32efe04cc28e275d3ac2188cad6a9f73544f3	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\IconCache.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	26.84 KB	4ad852039685b9bb57b2389fca685f3cb679fb0fdb559a6b0f114053a442d007	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\burn\burn\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	174 bytes	991b8cdcad4b772d077ea920454754e1f673b272b9d9c53b759c92b274bd3bd1	✖
-	1.19 KB	34f5ac9f1c5e53e0c9bea066fc2a067d411bb1c1709d1eee3d95751111ed1550	✖
-	2.35 KB	901e255a99e07e5e1163f91af407a06e7a9adb975d08d12b3c79210962ffd888	✖
-	16.00 KB	a40e1fd7a59eb903c24b975a3b4d304a85d7e346c4e424536e9344efe8717844	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	203 bytes	07c043acf2fff23864169d5fcd7a3e909ad62943df153b4897dce6cbca931d75	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (0) - 776 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	837 bytes	fb0b342824e076e3fd942fc913ae9a222a6a7079566e89de78f59eb07f0aaf6c	✖
-	16.00 KB	b372afbd59c93ccf0e6dc557f3e349bbeee5363019b5691c51849aee6afd1b8f	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	1.08 KB	598d59473bef88f7d71303e319f147400f53d9e451d8eeb698bee16af89409ff	✖
c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	148 bytes	3f25fa6777d33d813aefeea2f06746ef48567b0ba2fae6da5741603920431122	✖
-	337 bytes	6d96df67c0f31ae18725c7a8c10f91310de79c613f38cb3daef509ab0d167630	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\48415de7.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	3.84 KB	14769bd6da3efaf1850dbda77122e27d0e41ce33312ec854e7fae77e865077705	✖
c:\users\rdhj0cnfevzx\appdata\local\comms\unistoredb\uss.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	8.00 KB	9062e638604d3f2fe4dbfa9ca4388252e9e11aff251cc2c7e93af213d767c1c7	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{14280630-395B-4995-BD22-15BD491A464A} (1) - 3904 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	300 bytes	9c98d964075b7ac1eab2331c48a8978eb24b193f30a3033d6873ba35879883c15	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{7D881D02-986E-4A6B-893F-406DB8A8A682} (1) - 3440 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	300 bytes	5b4510e294f100f1111db51abe26a047d09c492056d0188ff65e68054bede88c	✖
-	55.99 KB	3484670b0cefad14466a5e81727fea1bfda6bb1b29076189ecb35a59ca3392bc	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\6bf71745.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	6.88 KB	237eb938657562e90441c099b9a57764508f68ee90d702d1d243e6687ca3def2	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\msvcp120.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	444.66 KB	259942e340eb5bf5599bf94299567825446 1a8567b810aab3971acdb536bb668	✖
-	80 bytes	1e2841020f6667ab5f4419f64f72246c5181a631ed7c7e8a9e5d5ea28265618b	✖

File Name	File Size	SHA256	YARA Match
-	2.63 KB	d22cc97442e5e81697a307db26ce82a10b58b8175873cb49089b8acdf5d931df	✖
-	1.09 KB	b05cd7ee25d57d6b134975d533f17b9d0a5d65c7824de4ee3ad326df2d8943de	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\C1J92J4X\2\C__Windows_SystemApps_Microsoft.Windows.Cortana_cw5n1h2txyewy_cache_COOBE_COOBE[1].html.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	17.84 KB	9a179d46ebd9bf1770216fe1f46baf2b4a6e30f63538d9289dea9e8c0055282a	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{76787746-0EF6-4759-84BC-631B78C93EB7} (0) - 3608 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	837 bytes	22032540a3548f1d2a6a0cd9a6ab58f05f9993448936137030c8b52b97008442	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_1280.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	24 bytes	8a547836f6368c05efb18a4084be8abe3e8d2f5b4d91fed5b809115574cccf6d	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{5ABD4B01-ABA3-41BD-9FD7-3DB72380D196} (1) - 3620 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	483 bytes	cfdf3701459893919ca45fb63f5d738b1ee92fa3db9d1e74b82744e7c0d6a1d8	✖
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\history\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	130 bytes	d01c77764c26915784a7627b1cc577db827184be3dee7464f3dfdbfee288180d	✖
-	1.02 KB	dc0c02a7d24fdd1dcd1a97327ff27844a9f49e72ee76bcad26d8ea468dde0162	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	24 bytes	e0cd8d4798f7fc413d28e41fb1c97051ee72e82db7992b6e0d96590877f22fb5	✖
-	85 bytes	738f08a5e8d6355f5314a3313a77f5c6c473f8e18eb0f27d21b120cf00f586e6	✖
-	188.00 KB	7bbb639a4d47af41b8afa62ea726c905fbf5c290f33c87ef015deec56e4a2ef4	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	4.12 KB	c4553b4cec4081cdc72b050840c1636db32e97c42505eeb8608a3b151833c8d9	✖
-	1.13 KB	624bc23b3e8eeb1028b910d806a92c3c2beb0ea1047d03c17242455b6cdbe5ad	✖
-	2.29 KB	d509e76d9ea1406f2a5a49a531b0068ee72db30de17f4d3b0f1e6ac8387daa7a	✖
-	337 bytes	81443b87cf66425f6fbb7ffbcee0db404ae259cf9991bf91edaa2582fcac3d90	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Uninstall-PerMachine_2022-08-03_151233_e44-b50.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	67.11 KB	b5ffd1983c06b0786bdbd44682659590c740232fa67379ad9f5c03d4fadbffc3	✖

Reduced dataset

Host Behavior

Type	Count
Module	7
Registry	2
Keyboard	2
Window	6
File	22202
System	3906

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f	C:\Users\RDhJ0CNFevzX\Desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	Sample File	172.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
dd8b85247f58a60c3a5e5153ea447e1ddc131c90f6969f027cfe42585256aabf	-	Dropped File	65.58 KB	application/octet-stream	-	CLEAN
880ccb2287431ea9c087e65357a00139a948142e991565529b72a572d77fc421	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{E347E1DF-602B-433D-B049-596C6048612B} (1) - 3128 - excel.exe - OTele.d... ...office\otele\{e347e1df-602b-433d-b049-596c6048612b} (1) - 3128 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	300 bytes	application/octet-stream	Access, Create, Write	CLEAN
5698bc5992fd3c04de7fe8fbbdf5322ecc61770a12ccd02df81dfa782d622907	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group2\1 - run.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\User... ..._xxx_xxx_xxx, c:\users\default\appdata\local\microsoft\windows\winx\group2\1 - run.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.08 KB	application/octet-stream	Access, Create, Write	CLEAN
a99fd5f8151bb0a569df634bbf878ef6034ba671d96ec74fb759a9b0e1c70685	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TCPrefs_2_D3E71568CFF98B44AA768B6125CC6184.dat.crypted_pony... ...ocal\microsoft\outlook\roamcache\stream_tcprefs_2_d3e71568cff98b44aa768b6125cc6184.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	204 bytes	application/octet-stream	Access, Create, Write	CLEAN
4c4fbe32af44be1ab54353fd29c569ebb74f53cb9b5f754e77b096b4d72d0fac	-	Dropped File	2.15 KB	application/octet-stream	-	CLEAN
fdc3fa4fef644c22b3aafc45c0d5a95fee2550d072e908747b05c729e53720bb	-	Dropped File	2.61 KB	application/octet-stream	-	CLEAN
5c515dce6537271ae3201088a32c06286385b2441f2f07ce17e93d3b22ed41a4	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\8L05D5LK\favicon[1].ico.crypted_pony_test_build_xxx_xxx_xxx_xxx... ...sers\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\8l05d5lk\favicon[1].ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	4.19 KB	application/octet-stream	Access, Create, Write	CLEAN
d10695f2975bb83a275dc9c32db753bce9cf8e6679b66a88e8199ae57141f8a7	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\AutoPlayLogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_x... ...\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\autoplaylogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	4.56 KB	application/octet-stream	Access, Create, Write	CLEAN
79e14823fc7b287e40c9cde214dc0568b461fdcbac15e463e44a9c66468e4c69	-	Dropped File	279 bytes	application/octet-stream	-	CLEAN
434ef515937a8b23637e8cbc429a6af4bb83be1c55f021853f2f8a14318abdbb	-	Dropped File	1.32 KB	application/octet-stream	-	CLEAN
0f778442f6e1a923a7a5b5680867a5ff7e4ed1dab49cd8ddd126eb03e87179b2	-	Dropped File	24.62 KB	application/x-dosexec	-	CLEAN
1169b27e51159cf5a43864824bf6a8b8149fc2173b76b8b1f7904bf9a4c520b7	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8c7f41e5b9996b3c5971690586b6140b4fa069f22664fe660a3add9c3e483ec4	-	Dropped File	2.02 KB	application/octet-stream	-	CLEAN
5068a913cbcbea91d534589133208c5f49bf02a10adf730b495b7dcb47dd1342	-	Dropped File	36.00 KB	application/octet-stream	-	CLEAN
0de6f0373b18c0f56efbeaf195e4fff613dc88a43f142dd46c0b7001518ec259	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{476867b0-6c71-41f9-b8ee-957d2c806c59} (0) - 3924 - winword.exe - otele... ...\{476867B0-6C71-41F9-B8EE-957D2C806C59} (0) - 3924 - winword.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	845 bytes	application/octet-stream	Access, Create, Write	CLEAN
e1dc8b5b9781389faff8509ec1b0b90c020024175ddc0be4dea2ab021c5ffbee	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\no... ...8bbwe\ac\microsoftedge\user\default\datastore\data\nouser1\120712-0049\dbstore\edb.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
b6ffd6114748daf719e683e5157f5f693c53b3511e1eeb3a4dab4245cbde20eb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\ScreenshotOptIn.png.crypted_pony_test_build_xxx_xxx_xxx_xx... ...ers\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_2\screenshotoptin.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	432.01 KB	application/octet-stream	Access, Create, Write	CLEAN
09493d5e3c3ad9da400da9056c2d1bda1da2778397392d84499a18b40273a4ba	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{12E262E7-D2B6-4D7F-8C8E-099A50A4E1B9} (0) - 3576 - excel.exe - OTeleMe... ...le\{12e262e7-d2b6-4d7f-8c8e-099a50a4e1b9} (0) - 3576 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	837 bytes	application/octet-stream	Access, Create, Write	CLEAN
2778f34525289a8c37c1ab3b878bee091a725caf6ad5a94810a6c471695a20bb	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{D32DDB02-A781-4D79-BBB3-90DD7781C33D} (0) - 3812 - excel.exe - OTele.d... ...office\otele\{d32ddb02-a781-4d79-bbb3-90dd7781c33d} (0) - 3812 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	279 bytes	application/octet-stream	Access, Create, Write	CLEAN
32cbf0c96a682b29e794e5849d27a5174b5543dab31a2c8288497af4825d30fa	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (1) - 3500 - excel.exe - OTeleMe... ...le\{bca15875-e8cf-40e2-a2a2-a665fc46f3a7} (1) - 3500 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	483 bytes	application/octet-stream	Access, Create, Write	CLEAN
84d6fa8848d73d97177f111e90d4721eb087da5904239b5f91b8de83301db947	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{6b789349-1698-4ea5-b0f1-2664e9e9ae46} (0) - 3248 - outlook.exe - otele... ...fice\OTele\{6B789349-1698-4EA5-B0F1-2664E9E9AE46} (0) - 3248 - outlook.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	283 bytes	application/octet-stream	Access, Create, Write	CLEAN
290c39cec9af73ba4405449968e229a190a4b48d3a9e6680f190cb4403f0a633a	-	Dropped File	790.79 KB	application/octet-stream	-	CLEAN
749c2df00d2de4fd377ef4e12b53156af4e72fcb795319e6905201c2c75fece6	-	Dropped File	24.62 KB	application/x-dosexec	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
75c22250be41a91bf3750d53022847de8fb7823bc41d3387309e338f73f9f546	c:\users\rdhj0cnfevzx\appdata\local\microsoft\gamedvr\knowngamelist.bin.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\GameDVR\KnownGameList.bin.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	52.56 KB	application/octet-stream	Access, Create, Write	CLEAN
a7b553052a80804cfdbbe078b26806f66dd8a9e1546728c7d78cfe4cd91042ad	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\caches\{3da71d5a-20cc-432f-a115-dfe92379e91f}.1.ver0x0000000000000019.db.cry... ...osoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.1.ver0x0000000000000019.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	42.64 KB	application/octet-stream	Access, Create, Write	CLEAN
589adacd2e368fe5b8373a8804e113b9371be823877888361b2f9138262e1cff	-	Dropped File	1.07 KB	application/octet-stream	-	CLEAN
5148fd2571e37bab89101c083257c8c320e93b102a19703cb0929e6f164cc3e7	-	Dropped File	80 bytes	application/octet-stream	-	CLEAN
17ded93d5a889df37a1eb181d4cbac2290440f61309c3fcb6416b0912ba4ff1d	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{5abd4b01-aba3-41bd-9fd7-3db72380d196} (0) - 3620 - excel.exe - otele.d... ...Office\OTele\{5ABD4B01-ABA3-41BD-9FD7-3DB72380D196} (0) - 3620 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	279 bytes	application/octet-stream	Access, Create, Write	CLEAN
7ce6bcdd5345c3fa8ccea25dc0ba908596d58774015f82a0f56b6bfb4032d39c	-	Dropped File	2.17 KB	application/octet-stream	-	CLEAN
990ad4e0cd0fe3b2ac439c70fd07e5becd7fbea4ad9845203bb06f27e76076df	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (0) - 3500 - excel.exe - OTeleMe... ...le\{bca15875-e8cf-40e2-a2a2-a665fc46f3a7} (0) - 3500 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	837 bytes	application/octet-stream	Access, Create, Write	CLEAN
04033a02c5debf8905cfb8f62dc74fb96ac47cbd5091a15f6165c7826031dedf	-	Dropped File	8.00 KB	application/octet-stream	-	CLEAN
8a9c3d0351db0261052f87ca0fc757a064ab75c08eccf099a4482f259b8172cc	c:\users\public\music\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\Public\Music\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	380 bytes	application/octet-stream	Access, Create, Write	CLEAN
7c0c08efaad1dd4d49abc41defd5e4118975eb1ef0d98ef24819dfe2df91ad50	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group3\07 - event viewer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xx... ...xx, c:\users\default\appdata\local\microsoft\windows\winx\group3\07 - event viewer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1015 bytes	application/octet-stream	Access, Create, Write	CLEAN
17a47251a683ad9e1a0205fe323935a4286f9a8576a18f8cded4b9e63901c0ad	-	Dropped File	2.05 KB	application/octet-stream	-	CLEAN
c69929e81cfd996d2e7622f0dd8aa270887c692419548ba420e6697cd59ca43d	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group3\09 - Mobility Center.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx... ... c:\users\default\appdata\local\microsoft\windows\winx\group3\09 - mobility center.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1015 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5d3313f0a40d350552b810ab8eadba1c8e79bf815139e47f62964e26c16c9bdf	-	Dropped File	2.54 KB	application/octet-stream	-	CLEAN
76843caf1a2a6f20d30b6a97b395abe60c302e2e8f2eb08409de7bb3d444e2a0	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN
ad1d99f65437b3db654dd2f172291e38bbb124b3616acb7816a3946ded18531a	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group3\01a - Windows PowerShell.lnk.crypted_pony_test_build_xxx_xxx_xxx... ...Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3\01a - Windows PowerShell.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.10 KB	application/octet-stream	Access, Create, Write	CLEAN
12c6336959a5657547cc1eb9b802444bc83955f348cee7040d248be440d4c966	-	Dropped File	1.44 KB	application/octet-stream	-	CLEAN
6b34f5d76ff3f3172e2d7cb3aebfc63a7fac773b8c433408b9cd1a944841cf0b	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Desktop.ini.crypted_pony_test_build_xxx_xxx_x... ...efault\appdata\roaming\microsoft\windows\start menu\programs\accessibility\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	568 bytes	application/octet-stream	Access, Create, Write	CLEAN
7fd8ca66fd6bd571edf16d1df8defe2e83a00a6b9492e5407136d8d0c250d41e	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install-PerUser_2021-02-11_132743_ca8-cac.log.crypted_pony_test_... ...data\local\microsoft\onedrive\setup\logs\install-peruser_2021-02-11_132743_ca8-cac.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	228.16 KB	application/octet-stream	Access, Create, Write	CLEAN
d9086ff50af6d4cc5aa20f04cf27440b3dc982e1a2cf7e01ecafa6d337f9ebf6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WebCache\V0100006.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\webcache\v0100006.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	512.00 KB	application/octet-stream	Access, Create, Write	CLEAN
4db88b0878e0229bcd3b16c54c5d1d665fbd476b31ad3e14b573c2ceb9b621c1	-	Dropped File	273.95 KB	application/octet-stream	-	CLEAN
6652121aa2f57251084487141 8e76f1a2dee8d66b76457881ce20d033043b669	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (0) - 776 - excel.exe - otele.da... ...\Office\OTele\{78AE2E81-404D-463F-8150-C93CDDA45E7B} (0) - 776 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	279 bytes	application/octet-stream	Access, Create, Write	CLEAN
b671338d996e3167c4010974540789c6cea877225b52d754d752d878453e1663	c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2txyewy\ac\appcache\c1j92j4x\2\c__windows_systemapps_... ...dows_SystemApps_Microsoft.Windows.Cortana_cw5n1h2txyewy_cache_COOBE_CortanaIcon[1].png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	6.44 KB	application/octet-stream	Access, Create, Write	CLEAN
a885c577a756ccc53cbb3750a8e4661b3663be6ff7bb1f3b65592bd2c990bc31	c:\users\default\appdata\local\microsoft\windows\winx\group2\5 - task manager.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\... ...C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group2\5 - Task Manager.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1021 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a19c7dee5d7125f4064ffd3396a688cee2ccf8effc4b5612db068b45eac9ff4b	-	Dropped File	1.13 KB	application/octet-stream	-	CLEAN
9e776a202f722bc6d5bc21e0e83ecc4a1abea40ebc5652f1406a9665cb922fb5	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\setup\logs\install_2021-02-11_131858_ed0-ed4.log.crypted_pony_test_build_xx... ...evzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install_2021-02-11_131858_ed0-ed4.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	61.49 KB	application/octet-stream	Access, Create, Write	CLEAN
4f7918bf6f1a9803e31a17207052d651787ac65ca2d9542e7c405cd610344a41	-	Dropped File	26.38 KB	application/octet-stream	-	CLEAN
5202b2e48f23d862cfe88822d95a06b250b7d70cc1f0124c1127ba7255e5ec22	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\27771a56.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\27771a56.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	13.40 KB	application/octet-stream	Access, Create, Write	CLEAN
db3926687491a281808b1c49448ad8c6ce3fa24b6f9f01bbc7f209ff9ec4626c	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{76787746-0ef6-4759-84bc-631b78c93eb7} (1) - 3608 - excel.exe - oteleme... ...le\{76787746-0EF6-4759-84BC-631B78C93EB7} (1) - 3608 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	483 bytes	application/octet-stream	Access, Create, Write	CLEAN
f0721cf077200d10bedbdec08bc125dbe7b114811c1508c0e484a3420eea35be	-	Dropped File	2.75 KB	application/octet-stream	-	CLEAN
55e31869385a48e41f801d55d738d70a97ce8d9e15dcff173accd8a1f4609769	-	Dropped File	1.10 KB	application/octet-stream	-	CLEAN
1ccdd07b99097fb5354465e2437bb13d330d89068a5b063d8f513265e453a452	-	Dropped File	501 bytes	application/octet-stream	-	CLEAN
aaabccbe093db361eebdebc2782e64ac3cfedb4e2ebbc46925a549db7b3ddcbf	-	Dropped File	321 bytes	application/octet-stream	-	CLEAN
fb9442838dfd009ffd6702a845ef225eecfc0b5e3bbc09364c66c167b66ce094	c:\users\public\pictures\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\Public\Pictures\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	380 bytes	application/octet-stream	Access, Create, Write	CLEAN
5f827696267e972210e77f8a2c4e701977888d28168a4ea9210b8c23dbeaeb2b	c:\users\default\appdata\local\microsoft\windows\winx\group2\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\Def... ...xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group2\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx_xxx	Dropped File	332 bytes	application/octet-stream	Access, Create, Write	CLEAN
bd46a765bd1141da6c435ddfcee132a9995391b44f92f26074297ffe33f28277	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{6b789349-1698-4ea5-b0f1-2664e9e9ae46} (0) - 3248 - outlook.exe - otele... ...\{6B789349-1698-4EA5-B0F1-2664E9E9AE46} (0) - 3248 - outlook.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	845 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
26af47bf402a2b22397015a4ebd300f143a4f348346b09f5b0b235237f372bdf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install_2021-02-11_132742_c8c-c90.log.crypted_pony_test_build_xx... ...evzx\appdata\local\microsoft\onedrive\setup\logs\install_2021-02-11_132742_c8c-c90.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	61.49 KB	application/octet-stream	Access, Create, Write	CLEAN
7399ec72b5418acc5941383263bf3313ae412c3da1f637e8ac0cb57c17ad3547	-	Dropped File	1.15 KB	application/octet-stream	-	CLEAN
09ec6613c930a2dcf20d0f79de079a49577f8df4573be319557774556d6d8a15	-	Dropped File	1.07 KB	application/octet-stream	-	CLEAN
a69eb3144eeb0b328a79757b545ce81822c1495b4a6743629e3a90ba60e99843	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_2\screenshotlogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx... ...sers\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_2\ScreenshotLogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	4.57 KB	application/octet-stream	Access, Create, Write	CLEAN
48adf118b5579fbee7495fc26f15593563779e64cf1688d82ba3e47791e5e5a2	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\autoplayoptin.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_... ...users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\autoplayoptin.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	374.24 KB	application/octet-stream	Access, Create, Write	CLEAN
b4c0a32297960ac68d6e536097c88ac5ad57193e31904dc1ed2c48c9a3e0e73b	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{C9F887AB-1565-4D03-878C-E985B67FFEF2} (0) - 3748 - excel.exe - OTeleMe... ...le\{c9f887ab-1565-4d03-878c-e985b67ffef2} (0) - 3748 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	837 bytes	application/octet-stream	Access, Create, Write	CLEAN
68404875ff629b362c1450d010501ee6a702ad96153c549f715ff0fba32071b8	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\amd64\filesyncapi64.dll.crypted_pony_test_build_xxx_xxx_xx... ...RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\amd64\FileSyncApi64.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	256.00 KB	application/octet-stream	Access, Create, Write	CLEAN
68b0b413e61e398d5218fa19e744d6137de19d86714c32df3a9673aa1d3c4925	-	Dropped File	56.95 KB	application/octet-stream	-	CLEAN
82f43f835574530d9a3e0fa086fcaab795e625910f05b56e6ab454eb8da10ccd	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.AccountsControl_cw5n1h2txyewy\Settings\settings.dat.crypted_pony_test_build... ...x\appdata\local\packages\microsoft.accountscontrol_cw5n1h2txyewy\settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
1b9278485b6e07398345bf09ae5a5de674ea8828ad20a53451682b25b1bdec4b	-	Dropped File	80 bytes	application/octet-stream	-	CLEAN
cd47ef02db9cc172f749290aea7613c94e030e083be604d03e9d93e4105bfbad	-	Dropped File	1.11 KB	application/octet-stream	-	CLEAN
f6db98c54e1e667137e9b6237a9d31d292a3a6fba456e025e3409530bb8fa399	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\7a67116a.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\7a67116a.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.26 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3f2720cf72e3f6aa6ea624f12323767ee85aa8250403bbd63f0eaff5d6efc844	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_256.db.crypted_pony_test_build_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Explorer\iconcache_256.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	24 bytes	application/octet-stream	Access, Create, Write	CLEAN
5889179ca119305e3ca0b8e7642491ed7ca549c016213c7a8b2e0711cc4999d1	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\ad9a3041.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\ad9a3041.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	9.63 KB	application/octet-stream	Access, Create, Write	CLEAN
1c88eb5a443c6ca1da71744a9e04d1cd595df17546e7fa3b6ba5319de26b481c	-	Dropped File	23.71 KB	application/octet-stream	-	CLEAN
5429c849aae1e5d4fba9b7d6d8fa2933741ab3628918a53ea7081002273c2b2c	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\collectonedrivelogs.bat.crypted_pony_test_build_xxx_xxx_xx... ...rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\collectonedrivelogs.bat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	5.71 KB	application/octet-stream	Access, Create, Write	CLEAN
3eacb83a8788b2f982b84ee980dc3704592c18603686746 2fa0d2d5a94189782	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Microsoft.BioEnrollment_10.0.10586.0_neutral__c... ....bioenrollment_10.0.10586.0_neutral__cw5n1h2txyewy\activationstore\activationstore.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
f1567047c2a4e0d3c9eeadfb1dacb54523a3e1c3baa2d689cd5d3087de535bcf	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WinX\Group1\1 - Desktop.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, c:\... ..._xxx_xxx, C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group1\1 - Desktop.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.08 KB	application/octet-stream	Access, Create, Write	CLEAN
10c76e5d4ba201b6e21821aca82ec4ea523ce9f6edc09d90f4ade5ad9af743fb	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.crypted_pony_test... ...oaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	2.18 KB	application/octet-stream	Access, Create, Write	CLEAN
0660b35b5e76bd8e47672ba6f59f01f888a64a4df12ab79713687cbb73140fb6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000017.db.cry... ...osoft\windows\caches\{afbf9f1a-8ee8-4c77-af34-c647e37ca0d9}.1.ver0x0000000000000017.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	108.52 KB	application/octet-stream	Access, Create, Write	CLEAN
9415ec8723d4eb0ba039de7d253b975ada536160bcc1c833a25f70e977152704	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\d242e6bf.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\d242e6bf.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	3.76 KB	application/octet-stream	Access, Create, Write	CLEAN
cb1885f879e3c4a687d849f925f0af2f676f31d7d2b2d9681f72b436163703f2	-	Dropped File	174 bytes	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c96c6ac9382646cc0b8d4b7fbeb630c52a50e4049bb25834da9731e01347fee9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\WnsClientApi.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_x... ...\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\wnsclientapi.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	373.69 KB	application/octet-stream	Access, Create, Write	CLEAN
924cbbcc1458a21ee226669035bff1e43dc88e6d6e50eef317f9f9784682a929	c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v4.0\usagelogs\sdiagnhost.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\sdiagnhost.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	5.47 KB	application/octet-stream	Access, Create, Write	CLEAN
23d9dc852ebb7a4a4dd44536d93aa658baf42b12a2d8fa3aa3f3f7232b91d41e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{730eed67-cb03-48eb-b6a2-97fadd6a81fb} (1) - 3644 - excel.exe - oteleme... ...le\{730EED67-CB03-48EB-B6A2-97FADD6A81FB} (1) - 3644 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	483 bytes	application/octet-stream	Access, Create, Write	CLEAN
ebd6d610da3a81064fa5a02e4f67897360d4d98726a6d64e54bff378043b381a	-	Dropped File	1.13 KB	application/octet-stream	-	CLEAN
a28bd09fd6fd841cbe32bb4f2413852be87187de62b1751a0430f3bb1dbb5a51	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{c9f887ab-1565-4d03-878c-e985b67ffef2} (0) - 3748 - excel.exe - otele.d... ...Office\OTele\{C9F887AB-1565-4D03-878C-E985B67FFEF2} (0) - 3748 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	279 bytes	application/octet-stream	Access, Create, Write	CLEAN
4294b13411128402379 44a465c1ce01c4ce5d6d7522f5311b1f6c57120949602	-	Dropped File	1.22 KB	application/octet-stream	-	CLEAN
aa0f6793182693f1c5935ce40936bc0cbf8e4e35c47e9deea4411eebb634029f	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppData\Indexed DB\edb.chk.crypted_pony_test_... ...data\local\packages\microsoft.windows.cortana_cw5n1h2txyewy\appdata\indexed db\edb.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
2d0190c56cb97dedcb945567ecdfba6a744cdb588d9e631320565dde0d1c45fb	-	Dropped File	4.55 KB	application/octet-stream	-	CLEAN
e31a854a6e7ade7e9b7deb646732319d53a22888c9501c653adee28ca68f7b15	c:\users\default\appdata\local\microsoft\windows\winx\group3\08 - power options.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C... ...\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group3\08 - power options.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.05 KB	application/octet-stream	Access, Create, Write	CLEAN
d3a704d07e3d5e9bb7dd5bded4768aff2abdfd9b542e82501e09fc24e519c624	-	Dropped File	50.67 KB	application/octet-stream	-	CLEAN
7fa76e5d0760b346db219545bf9338b7bf550eaa59dac77c8c94789d3f01236f	-	Dropped File	1.08 KB	application/octet-stream	-	CLEAN
88a6735ddad1e5b5c5a24b9982192c35a23e01981c208dbd865b1c24961fce6a	-	Dropped File	1.21 KB	application/octet-stream	-	CLEAN
45fb24d33c298625bae626d59a396bbdf3416ce20b4d99f8de74c36e2a7f0a3f	-	Dropped File	24.62 KB	application/x-dosexec	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9556b3501bfa33db5e3e33f700ea0336f51d99dd9d847d1c8619558eb4b45600	-	Dropped File	576 bytes	application/octet-stream	-	CLEAN
39651697284635c4106cdf83337f08f1c0d5286b7a78cf76bc2d3ef42b4e75df	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\no... ...microsoftedge\user\default\datastore\data\nouser1\120712-0049\dbstore\logfiles\edb.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	512.00 KB	application/octet-stream	Access, Create, Write	CLEAN
6c395c0c431a0cfdb74ecf5049feee26fda38b6179f3a5d7b4451fff20884231	-	Dropped File	433 bytes	application/octet-stream	-	CLEAN
96ac84ebc21a1f9d96344d59cebcab2df960eb27764a51a087bfea69800bb2c0	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN
06ff150994ab9839e3cbe38d672996055d2430bd9eed1844ec1d5b15053b9daa	-	Dropped File	25 bytes	application/octet-stream	-	CLEAN
49b47fa1845aa1397758b1fbddae07f9c019cb4e5caab675b6745acf7bdea590	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN
efacb2bc8c3792644bbd4e77e4afbe503dfb6d918646c030ec6defdef66754ed	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{d32ddb02-a781-4d79-bbb3-90dd7781c33d} (1) - 3812 - excel.exe - oteleme... ...le\{D32DDB02-A781-4D79-BBB3-90DD7781C33D} (1) - 3812 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	483 bytes	application/octet-stream	Access, Create, Write	CLEAN
b927713d723501d5675db7c55dc8aed2c1d71d31513b7ce4ba6ae71a7242e027	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (1) - 776 - excel.exe - otele.da... ...\Office\OTele\{78AE2E81-404D-463F-8150-C93CDDA45E7B} (1) - 776 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	300 bytes	application/octet-stream	Access, Create, Write	CLEAN
93566382ffb4877867811a5264163e9aa5d1ece5f0b71b9a3d09164e96708aae	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{5abd4b01-aba3-41bd-9fd7-3db72380d196} (1) - 3620 - excel.exe - otele.d... ...Office\OTele\{5ABD4B01-ABA3-41BD-9FD7-3DB72380D196} (1) - 3620 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	300 bytes	application/octet-stream	Access, Create, Write	CLEAN
f5a696c9b8ca7d8e31b50bc134a151846c7e8fb7cadc0dac0a878ed32c057fbf	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN
c7752f8fca7285fd88d8400159cd4becd1d5c27dbc43ab04b931704d67306274	-	Dropped File	59.11 KB	application/octet-stream	-	CLEAN
9819287e541cd37e0b07a5a055bba354095653f9b92220872db71887344633a3	-	Dropped File	52.16 KB	application/octet-stream	-	CLEAN
fa11ceaa96b6365347e39954d732d4f1ef833c028ca41a8c6758dd828dd1e2d2	-	Dropped File	1.19 KB	application/octet-stream	-	CLEAN
2470ba7575d8189fdcf21f2ae5c45191297a85d8e3dda8b1c3b7b50f5b7c44c3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Uninstall-PerUser_2022-08-03_151233_600-778.log.crypted_pony_tes... ...ta\local\microsoft\onedrive\setup\logs\uninstall-peruser_2022-08-03_151233_600-778.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	71.83 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
73e6a5abf7883180bf336661522acb637ecec3daa4038950c452900b50e0db32	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.BioEnrollment_cw5n1h2txyewy\Settings\settings.dat.crypted_pony_test_build_x... ...vzx\appdata\local\packages\microsoft.bioenrollment_cw5n1h2txyewy\settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
863d083bb71490e9b7ec028b449e16dd5216314b4e47613ebe43d14b75ece2d9	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.crypted_pon... ... \Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell (x86).lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	2.18 KB	application/octet-stream	Access, Create, Write	CLEAN
ac6db52f08cac4da3c4fdadc38c992a093ed8a8f03f3e742e5e860e65321787d	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell ISE (x86).lnk.crypted... ...rosoft\windows\start menu\programs\windows powershell\windows powershell ise (x86).lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.24 KB	application/octet-stream	Access, Create, Write	CLEAN
29b8514225d66f3cad0ab6132797d2ac9a4d1bdfbe17eb35eeb612f121e5c553	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\webcache\v01.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\WebCache\V01.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN
d07a0cca26057dc9f0be31af8073f428229aaf95aa1538ab07e41c69b7d0d7b1	-	Dropped File	72 bytes	application/octet-stream	-	CLEAN
4bd5f4a03ec6dd970f539216d8af66b118ad3d253caf99a09695b2fe791f4ed8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Internet Explorer\ie4uinit-UserConfig.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...: \users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\ie4uinit-userconfig.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.27 KB	application/octet-stream	Access, Create, Write	CLEAN
bfeb06eed1776000a07912b8486eeb50569f0a739a88b1049b97be40d7828cae	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (0) - 3500 - excel.exe - OTele.d... ...office\otele\{bca15875-e8cf-40e2-a2a2-a665fc46f3a7} (0) - 3500 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	279 bytes	application/octet-stream	Access, Create, Write	CLEAN
54d8197589535f2046a4f1c552e32efe04cc28e275d3ac2188cad6a9f73544f3	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\1ced2593.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...: \users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\1ced2593.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	4.57 KB	application/octet-stream	Access, Create, Write	CLEAN
4ad852039685b9bb57b2389fca685f3cb679fb0fdb559a6b0f114053a442d007	C:\Users\RDhJ0CNFevzX\AppData\Local\IconCache.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\iconcache.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	26.84 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
991b8cdcad4b772d077ea920454754e1f673b272b9d9c53b759c92b274bd3bd1	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\burn\burn\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\... ..._xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\burn\burn1\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	174 bytes	application/octet-stream	Access, Create, Write	CLEAN
34f5ac9f1c5e53e0c9bea066fc2a067d411bb1c1709d1eee3d95751111ed1550	-	Dropped File	1.19 KB	application/octet-stream	-	CLEAN
901e255a99e07e5e1163f91af407a06e7a9adb975d08d12b3c79210962ffd888	-	Dropped File	2.35 KB	application/octet-stream	-	CLEAN
a40e1fd7a59eb903c24b975a3b4d304a85d7e346c4e424536e9344efe8717844	-	Dropped File	16.00 KB	application/octet-stream	-	CLEAN
07c043acf2fff23864169d5fcd7a3e909ad62943df153b4897dce6cbca931d75	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\addinutil.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v2.0\usagelogs\addinutil.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	203 bytes	application/octet-stream	Access, Create, Write	CLEAN
fb0b342824e076e3fd942fc913ae9a222a6a7079566e89de78f59eb07f0aaf6c	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (0) - 776 - excel.exe - otelemed... ...ele\{78AE2E81-404D-463F-8150-C93CDDA45E7B} (0) - 776 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	837 bytes	application/octet-stream	Access, Create, Write	CLEAN
b372afbd59c93ccf0e6dc557f3e349bbeee5363019b5691c51849aee6afd1b8f	-	Dropped File	16.00 KB	application/octet-stream	-	CLEAN
598d59473bef88f7d71303e319f147400f53d9e451d8eeb698bee16af89409ff	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.crypted_pony_test_buil... ...ata\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\On-Screen Keyboard.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	1.08 KB	application/octet-stream	Access, Create, Write	CLEAN
3f25fa6777d33d813aefeea2f06746ef48567b0ba2fae6da5741603920431122	c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	148 bytes	application/octet-stream	Access, Create, Write	CLEAN
6d96df67c0f31ae18725c7a8c10f91310de79c613f38cb3daef509ab0d167630	-	Dropped File	337 bytes	application/octet-stream	-	CLEAN
14769bd6da3efaf1850dbda77122e27d0e41ce33312ec854e7fae77e86507705	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\48415de7.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\48415de7.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	3.84 KB	application/octet-stream	Access, Create, Write	CLEAN
9062e638604d3f2fe4dbfa9ca4388252e9e11aff251cc2c7e93af213d767c1c7	c:\users\rdhj0cnfevzx\appdata\local\comms\unistoredb\uss.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Comms\UnistoreDB\USS.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	8.00 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9c98d964075b7ac1eab2331c48a8978eb24b193f30a3033d6873ba3587983c15	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{14280630-395B-4995-BD22-15BD491A464A} (1) - 3904 - excel.exe - OTele.d... ...office\otele\{14280630-395b-4995-bd22-15bd491a464a} (1) - 3904 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	300 bytes	application/octet-stream	Access, Create, Write	CLEAN
5b4510e294f100f1111db51abe26a047d09c492056d0188ff65e68054bede88c	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{7D881D02-986E-4A6B-893F-406DB8A8A682} (1) - 3440 - excel.exe - OTele.d... ...office\otele\{7d881d02-986e-4a6b-893f-406db8a8a682} (1) - 3440 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	300 bytes	application/octet-stream	Access, Create, Write	CLEAN
3484670b0cefad14466a5e81727fea1bfda6bb1b29076189ecb35a59ca3392bc	-	Dropped File	55.99 KB	application/octet-stream	-	CLEAN
237eb938657562e90441c099b9a57764508f68ee90d702d1d243e6687ca3def2	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\6bf71745.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xx... ...:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\6bf71745.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	6.88 KB	application/octet-stream	Access, Create, Write	CLEAN
259942e340eb5bf5599bf942995678254461a8567b810aab3971acdb536bb668	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\msvcp120.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, ..., c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_2\msvcp120.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	444.66 KB	application/octet-stream	Access, Create, Write	CLEAN
1e2841020f6667ab5f4419f64f72246c5181a631ed7c7e8a9e5d5ea28265618b	-	Dropped File	80 bytes	application/octet-stream	-	CLEAN
d22cc97442e5e81697a307db26ce82a10b58b8175873cb49089b8acdf5d931df	-	Dropped File	2.63 KB	application/octet-stream	-	CLEAN
b05cd7ee25d57d6b134975d533f17b9d0a5d65c7824de4ee3ad326df2d8943de	-	Dropped File	1.09 KB	application/octet-stream	-	CLEAN
9a179d46ebd9bf1770216fe1f46baf2b4a6e30f63538d9289dea9e8c0055282a	C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\C1J92J4X\2\C__Windows_SystemApps_... ...__windows_systemapps_microsoft.windows.cortana_cw5n1h2txyewy_cache_coobe_coobe[1].html.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	17.84 KB	application/octet-stream	Access, Create, Write	CLEAN
22032540a3548f1d2a6a0cd9a6ab58f05f99934489361370 30c8b52b97008442	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{76787746-0EF6-4759-84BC-631B78C93EB7} (0) - 3608 - excel.exe - OTeleMe... ...le\{76787746-0ef6-4759-84bc-631b78c93eb7} (0) - 3608 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	837 bytes	application/octet-stream	Access, Create, Write	CLEAN
8a547836f6368c05efb18a4084be8abe3e8d2f5b4d91fed5b809115574cccf6d	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_1280.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\U... ...xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	24 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cfdf3701459893919ca45fb63f5d738b1ee92fa3db9d1e74b82744e7c0d6a1d8	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{5ABD4B01-ABA3-41BD-9FD7-3DB72380D196} (1) - 3620 - excel.exe - OTeleMe... ...le\{5abd4b01-aba3-41bd-9fd7-3db72380d196} (1) - 3620 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	483 bytes	application/octet-stream	Access, Create, Write	CLEAN
d01c77764c26915784a7627b1cc577db827184be3dee7464f3dfdbfee288180d	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\history\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\History\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	130 bytes	application/octet-stream	Access, Create, Write	CLEAN
dc0c02a7d24fdd1dcd1a97327ff27844a9f49e72ee76bcad26d8ea468dde0162	-	Dropped File	1.02 KB	application/octet-stream	-	CLEAN
e0cd8d4798f7fc413d28e41fb1c97051ee72e82db7992b6e0d96590877f22fb5	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Explorer\iconcache_sr.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_sr.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	24 bytes	application/octet-stream	Access, Create, Write	CLEAN
738f08a5e8d6355f5314a3313a77f5c6c473f8e18eb0f27d21b120cf00f586e6	-	Dropped File	85 bytes	application/octet-stream	-	CLEAN
7bbb639a4d47af41b8afa62ea726c905fbf5c290f33c87ef015deec56e4a2ef4	-	Dropped File	188.00 KB	application/octet-stream	-	CLEAN
c4553b4cec4081cdc72b050840c1636db32e97c42505eeb8608a3b151833c8d9	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\powershell.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx... ...c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v4.0_32\usagelogs\powershell.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File	4.12 KB	application/octet-stream	Access, Create, Write	CLEAN
624bc23b3e8eeb1028b910d806a92c3c2beb0ea1047d03c17242455b6cdbe5ad	-	Dropped File	1.13 KB	application/octet-stream	-	CLEAN
d509e76d9ea1406f2a5a49a531b0068ee72db30de17f4d3b0f1e6ac8387daa7a	-	Dropped File	2.29 KB	application/octet-stream	-	CLEAN
81443b87cf66425f6fbb7ffbce0db404ae259cf9991bf91edaa2582fcac3d90	-	Dropped File	337 bytes	application/octet-stream	-	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_48.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\270n1ChiZI_1.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\3Fk41qKybaiEKn.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\C1J92J4X\8\container.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\all users\microsoft\windows defender\support\mpdetection-02112021-121950.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\tMlj6-2of.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\fbcb0eywdbm.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_2\SqmWrapper.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\AC\AppCache\C1J92J4X\6\container.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\INetCache\IE\8L05D5LK\favicon[1].ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu places\04 - downloads.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\nehll.mkv.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_2\filesync.localizedresources.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents_7kx8h\vd4qbai\eh1jpmpeo46ag.doc.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu\programs\java\check for updates.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\vgeijtkeri.avi.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu\programs\publisher 2016.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\OJKcISn3d2BAzwlafETu.bmp.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\6MHrGlVxhYS.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents_7kx8h\VD4qBAi\ZhhStph4\10Dj0NoHfl1fRCzJ80-K\fxGkChym_qpotd.rtf.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Notifications\wpnidm\1ba49cb8.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3\07 - Event Viewer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents_7kx8h\7IbgTAC0tGktM8kIYBG.doc.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\localstate\contentmanagementsdk\creatives\202914\eventbeacons.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\appdata\local\temp\xc64zb-20220802-1035.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\ast1nnrins.avi.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\recovery\active\{b20a1eca-2d21-11ed-b0cf-7896845e3b84}.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\jawshtml.html.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{c9f887ab-1565-4d03-878c-e985b67ffef2} (0) - 3748 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\dTBWs5OPc_Ez8klubHY.ots.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\-FRX5OOzUmfVjJcHf_DE.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\setup\logs\2021-02-18_130550_474-cac.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_9CB11E4EC4310E4C8A521398899F6363.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\pictures.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\office\recent\index.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\gen_py\3.8__init__.py.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\start menu\programs\accessories\notepad.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{BCA15875-E8CF-40E2-A2A2-A665FC46F3A7} (0) - 3500 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\ac\inetcookies\container.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\mnnvfs8uvolcl.flv.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\device stage\device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\notifications\wpnidm\8b8a3111.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\6mhrglvxhys\xrz0crxkdw.bmp.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell ise.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{78ae2e81-404d-463f-8150-c93cdda45e7b} (0) - 776 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Internet Explorer\Recovery\Active\{B80A0BDD-2D21-11ED-B0CF-7896845E3B84}.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Outlook\RoamCache\Stream_ConversationPrefs_2_CB6E3F7FAEA44A4FA14976E46D022840.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\Office\AssetLibrary.ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\downloads\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\actioncentercache\{3791ffdb-0f9b-43e7-b1bc-f83be99be18c}.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_4\amd64\FileSyncShell64.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{76787746-0EF6-4759-84BC-631B78C93EB7} (1) - 3608 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install_2021-02-11_134547_2bc-868.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.photos_8wekyb3d8bbwe\settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\bcemh oplek6-vr.bmp.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.accountscontrol_cw5n1h2txyewy\microsoft.accountscontrol_10.0.10586.0_neutral__cw5n1h2txyewy\activationstore\activationstore.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.XboxIdentityProvider_cw5n1h2txyewy\Settings\settings.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group3\02 - command prompt.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2txyewy\ac\microsoft\internet explorer\domstore\container.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Tyk8QAxzpbww82WIk.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu\programs\microsoft office 2016 tools\database compare 2016.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\uuLOLCY.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\nr0icrsgwqmcpon9gz.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\bjw1-4tbmjzvestfs.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\khe4uwhpks4.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\start menu\programs\accessibility\narrator.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group3\01 - command prompt.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents_7kx8h\vd4qbai\zhhstph4\tmlj6-2of.docx.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\xktgjsca6wfs.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\cltviflcleios.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{14280630-395B-4995-BD22-15BD491A464A} (0) - 3904 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\localstate\contentmanagementsdk\creatives\202911\imprbeacons.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\v4YCbLNj.rtf.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\2kvs--9w1i7hqqg.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\powershell.exe.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\202914\imprbeacons.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\internet explorer\quick launch\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2txyewy\appdata\indexed db\edb00040.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\diagnosis\parse.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\IEEEJcQHB4cvJ_cdO_.flv.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.LockApp_cw5n1h2txyewy\Microsoft.LockApp_10.0.10586.0_neutral__cw5n1h2txyewy\ActivationStore\ActivationStore.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\caches\cversions.1.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Character Map.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\filesyncshell.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\v-hs0zfeo.pps.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\office\mysite.ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Caches\{286DD990-B905-4D30-88C9-B63C603DA134}.3.ver0x0000000000000001.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\caches\{e23b5da4-e3a9-461b-8050-8e471867b572}.2.ver0x0000000000000001.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\webcache\v01tmp.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Uninstall-PerUser_2022-08-03_151233_600-778.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\vd4qbai.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\FThXpfrBZPMJLX.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\sbgkcoi59b4.jpg.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\recovery\active\recoverystore.{aabf9bf1-2d21-11ed-b0cf-7896845e3b84}.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\BdHdcndlyia--o2TJO\cdad4T_Z0CG2NFrmq2Q.avi.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_3\autoplayoptin.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\z5y0bnviuyw9okswr.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\vlzdvw69dnfcp zkr.flv.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\device stage\task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\ringtones.ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\all users\microsoft\windows\start menu\programs\accessories\xps viewer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Administrative Tools\System Configuration.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\BRFxsko.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\6MHrGlVxhYS\9xZXlJPvpfTMPJSEH.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\edb.chk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{D32DDB02-A781-4D79-BBB3-90DD7781C33D} (0) - 3812 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Package Cache\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}v11.0.61030\packages\vcRuntimeMinimum_x86\vc_runtimeMinimum_x86.msi.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEdge_iecompat\container.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\local\microsoft\windows\winx\group2\3 - windows explorer.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\thumbcache_custom_stream.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\device stage\task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\scan_property.ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{78AE2E81-404D-463F-8150-C93CDDA45E7B} (1) - 776 - excel.exe - OTeleMediumCost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\start menu\programs\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{7d881d02-986e-4a6b-893f-406db8a8a682} (1) - 3440 - excel.exe - otelemediumcost.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\package cache\{eea66967-97e2-4561-a999-5c22e3cde428}v14.25.28508\packages\vcruntimeminimum_amd64\cab1.cab.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_2\AutoPlayLogo.png.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{12e262e7-d2b6-4d7f-8c8e-099a50a4e1b9} (0) - 3576 - excel.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents_7kx8h\VD4qBAi\ZhhStph4\10Dj0NoHfl1fRCzJ80-K\8gkv\IzC9E.pps.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\All Users\Microsoft\Office\MySharePoints.ico.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu\programs\miracastview.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Searches\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\Windows\Start Menu\Programs\Accessibility\Speech Recognition.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\All Users\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows\start menu\programs\immersive control panel.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\explorer\iconcache_256.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\Windows\Start Menu Places\08 - Homegroup.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Office\OTele\{E347E1DF-602B-433D-B049-596C6048612B} (1) - 3128 - excel.exe - OTele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\Telemetry.dll.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\mEKNibmQaSlDxF.bmp.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Local\Microsoft\Windows\WinX\Group3\09 - Mobility Center.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Microsoft\SmsRouter\MessageStore\SmsInterceptStore.db.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\bdhdcndlyia--o2tjo\t7nndb1tqdapy7tj.mkv.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\setup\logs\Install-PerUser_2021-02-11_125336_9c0-9f8.log.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\bolZ.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\209857\imprbeacons.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\default\appdata\local\microsoft\windows\winx\group3\03 - computer management.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\bjw1-4tbmjzves tfs.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\all users\microsoft\windows defender\support\mpwpptracing-02112021-124618-00000003-ffffffff.bin.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\winx\group2\4 - control panel.lnk.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\6MHrGlVxhYS\qJQGc1JIO8.gif.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File, Modified File, Not Extracted	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{6b789349-1698-4ea5-b0f1-2664e9e9ae46} (0) - 3248 - outlook.exe - otele.dat.crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	cvtres.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	cvtres.exe	CLEAN

Process

Process Name	Commandline	Verdict
9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9ee11e680b1781159a9dac27566e45051dbe3016ff272f1d9c17cdf658e2ed7f.exe"	MALICIOUS
cvtres.exe	C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe	SUSPICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.2.24 / 2022-09-07 15:06:41
Link Detonation Heuristics Version	4.6.2.24 / 2022-09-07 15:06:41
Smart Memory Dumping Rules Version	4.6.2.24 / 2022-09-07 15:06:41
Config Extractors Version	4.6.2.26 / 2022-09-09 12:20:50
Signature Trust Store Version	4.6.2.24 / 2022-09-07 15:06:41
VMRay Threat Identifiers Version	4.6.2.26 / 2022-09-09 12:20:50
YARA Built-in Ruleset Version	4.6.2.26

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

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

System Root	C:\Windows