MALICIOUS

Classifications: Backdoor | Ransomware | Spyware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe**
ID	#4176417
MD5	057aad993a3ef50f6b3ca2db37cb928a
SHA1	a57592be641738c86c85308ef68148181249bc0b
SHA256	dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876
File Size	1839.00 KB
Report Created	2022-04-23 15:57 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 53 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe renames multiple user files.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: AbleFTP, Total Commander, git, The Bat!, Internet Explorer / Edge.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	Discovery	Reads certificate data	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe reads certificate "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\systemcertificates\my\appcontainerusercertread" from the file system.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Data Collection	Reads sensitive ftp data	2	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to read sensitive data of ftp application "AbleFTP" by file. • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Network Connection	Sets up server that accepts incoming connections	2	Backdoor
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe starts a TCP server listening on port 49713. • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe starts a TCP server listening on port 49715.			
1/5	System Modification	Modifies operating system directory	2	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe creates file "C:\Windows\Temp\satan\satan0" in the OS directory. • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe creates file "C:\Windows\Temp\satan\satan1" in the OS directory.			
1/5	Hide Tracks	Creates process with hidden window	2	-

Score	Category	Operation	Count	Classification
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe starts (process #2) cmd.exe with a hidden window. • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe starts (process #4) cmd.exe with a hidden window.			
1/5	Hide Tracks	Changes folder appearance	28	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\accountpictures". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\desktop". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\documents". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\downloads". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\libraries". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\pictures". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\videos". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public\music". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\public". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\internet explorer\quick launch". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\contacts". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\desktop". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\downloads". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites\links". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\links". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\music". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\onedrive". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\saved pictures". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\saved games". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\searches". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\videos". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe changes the appearance of folder "c:\users".		
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe resolves 88 API functions by name.			
1/5	Obfuscation	The binary file was created with a packer	1	-
	• File "C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe" is packed with "UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser".			
1/5	Network Connection	Performs DNS request	2	-
	• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe resolves host name "api.telegram.org" to IP "149.154.167.220". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe resolves host name "extreme-ip-lookup.com" to IP "37.48.65.182".			
1/5	Network Connection	Connects to remote host	4	-

Score	Category	Operation	Count	Classification
		• (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe accepts an incoming TCP connection from host "37.48.65.182:80". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe accepts an incoming TCP connection from host "149.154.167.220:443". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe opens an outgoing TCP connection to host "37.48.65.182:80". • (Process #1) dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe opens an outgoing TCP connection to host "149.154.167.220:443".		

Mitre ATT&CK Matrix

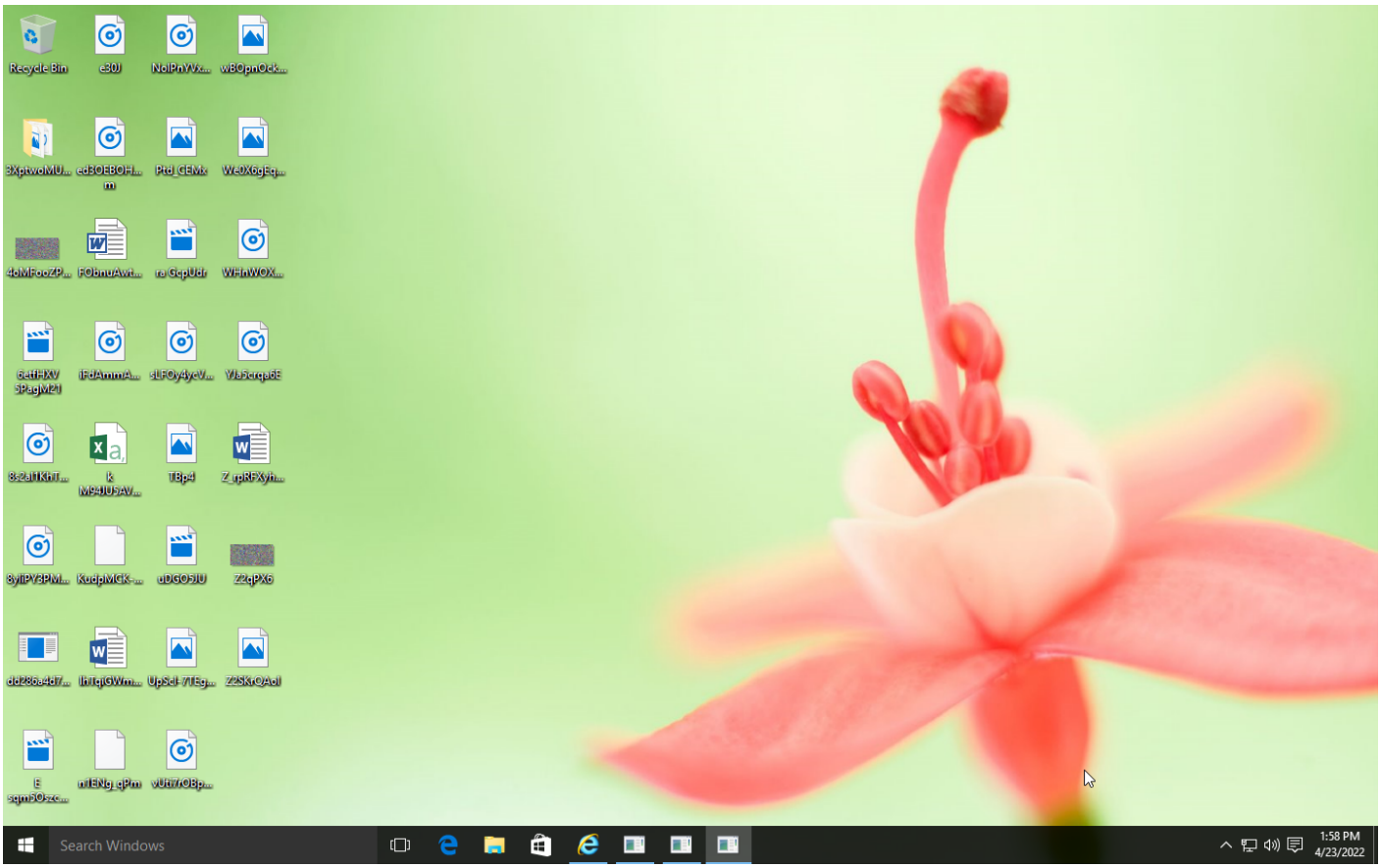
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
				#T1143 Hidden Window		#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1036 Masquerading		#T1082 System Information Discovery					
				#T1045 Software Packing							
				#T1027 Obfuscated Files or Information							

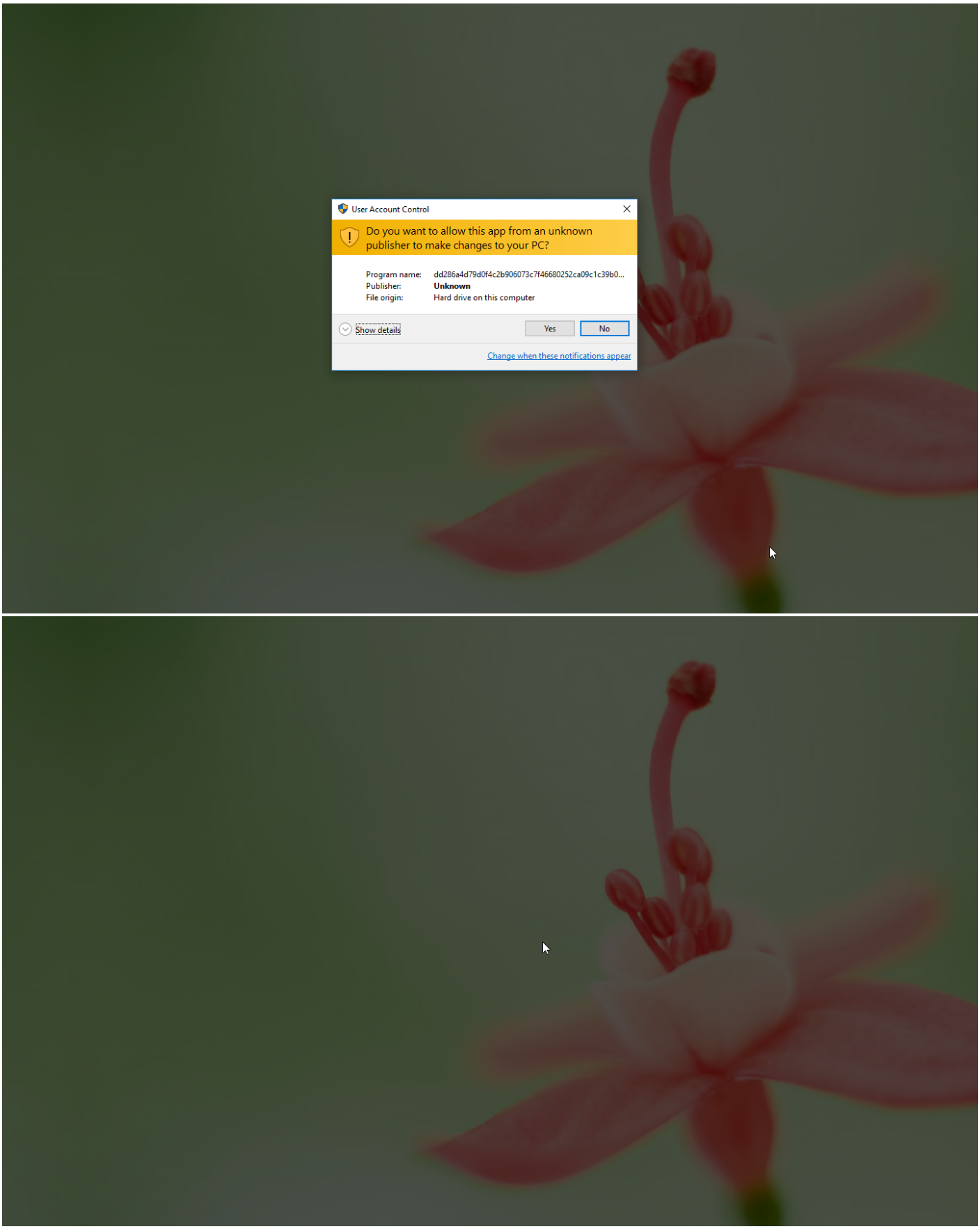
Sample Information

ID	#4176417
MD5	057aad993a3ef50f6b3ca2db37cb928a
SHA1	a57592be641738c86c85308ef68148181249bc0b
SHA256	dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876
SSDeep	49152:BY/3BNLViG5jQWArXncSxhBfV7xLE1t+XgWJz5qtAj6R:BwgG5MWMX7h8+Uw
ImpHash	406f4cbdf82bde91761650ca44a3831a
File Name	dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe
File Size	1839.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-04-23 15:57 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	3
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
Search Windows
1:58 PM
4/23/2022



Screenshots truncated

NETWORK

General

54.04 KB total sent

132.67 KB total received

2 ports 80, 443

3 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 2 servers

2 sessions, 1.73 KB sent, 46.04 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://extreme-ip-lookup.com/json/	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.telegram.org	NoError	149.154.167.220		NA
A	extreme-ip-lookup.com	NoError	37.48.65.182, 109.236.91.3		NA

BEHAVIOR

Process Graph

Process #1: dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 78620, Reason: Analysis Target
Unmonitor End Time	End Time: 319622, Reason: Terminated by Timeout
Monitor duration	241.00s
Return Code	Unknown
PID	1220
Parent PID	1184
Bitness	32 Bit

Dropped Files (162)

File Name	File Size	SHA256	YARA Match
C:\Windows\Temp\satan\satan0	184 bytes	40a77853e809080aa64cfd7581b67ad54ede1471c1be2cd1cedf60dd721064fc	✗
C:\Windows\Temp\satan\satan1	1.17 KB	fe9a642e4f0024a4958c7e2dbf6011a4c22c7f17abb984bdcad33beb6fa50706	✗
C:\\# SATAN CRYPTOR #.hta	4.38 KB	1b5681a1781363578f2a7fa2726e9a072f75f231ad028d967a4c8badd06fa7b4	✗
C:\BOOTNXT	631 bytes	81b62a4a6aa5bdde76a1add523b018ccd69414a9c559e8a073eeaa9383545fed	✗
C:\Boot\BOOTSTAT.DAT	64.62 KB	55100ff930a6edf6bbd1d3abb6f9f248d3b554f7c3824274b599c142cbf18cb2	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\MasterDescriptor.x-none.xml	21.15 KB	01a67420abd3dc877f950b44abc31323259cbc8285b4e21910f24fdfb33ff5b4	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\s321033.hash	732 bytes	e8c2ece5a9e70556322dc6cc741422cfcd27be3394939deb38764e8f3b92e38c	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\MasterDescriptor.en-us.xml	22.46 KB	84b9b51439a6e62ae6786efce8b379405411be55f4bab3d59d81f1ec204bb879	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\stream.x86.en-us.man.dat	865.07 KB	b0de407bd3639b5310584a30f2f067a41e7ce6c9f0090787eb34ebf47534f61c	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\s320.hash	732 bytes	94e068068fa00f84f8f9b7f701a2682349bff9944ac4bfdd0b8830cf7b7e8bec	✗
C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\stream.x86.x-none.man.dat	3630.07 KB	42a934bee260294e880736d02f166c116247a1bbabcd8de2504234eafd5a7a42	✗
C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.2.xml	1.96 KB	0c88423b0e76dd3f192b08db9dbd104a7e2c9217d507ab883259be7aed02fe21	✗
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserDeploymentConfiguration.xml	1.21 KB	7de3143aee32413b182d2865c787794cb8e53c855097f6136c3dce37e706a1a4	✗
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\DeploymentConfiguration.xml	1.21 KB	4e4bad77cdbb1e548548ce69fbbb8e513b8105d8682f9c9f6f14dfbd87572906	✗
C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.0.xml	2.54 KB	ddfcd5ee896d4662e1822836e95c2094da0a649626a940c8aeeba6044e1bb3f8	✗
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\Manifest.xml	4818.63 KB	782fd03b2cd8ef112d2a329c4e605c4b5342f4540684f832ad9c8b0167fd82fb	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserManifest.xml	3024.87 KB	a92291e624ef772551e097e2761beb3ec855d7894df088d982e002d4653bad25	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\AirSpace.Etw.man	276.15 KB	bd788b7af960f362372981945 57e666cbb05f29ff721473aae0ad68bf921ed35	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Access.Access.x-none.msi.16.x-none.xml	38.50 KB	23677d36bb54beac4a905aa7877f2f658c04df3f16724842348524e73ff46b88	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.DCF.DCF.x-none.msi.16.x-none.xml	16.88 KB	bb768bfc920d1c19e769b3bb9a6bb38d0a3906024a5b7714383a24b236bf84b7	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Excel.Excel.x-none.msi.16.x-none.xml	232.91 KB	86a40103ab163cc37c27454f60311e9542df63a36cba7933864df384a64f9aaf	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Lync.Lync.x-none.msi.16.x-none.xml	88.07 KB	d330bce45795685ab9f82c82695380b0d0bfa6370b86efe947698001c43d9f4a	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSMUX.OSMUX.x-none.msi.16.x-none.xml	2.86 KB	c4681417281899ca230de5269345bb499651c95ebe0621091a0136aa51a9fa58	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OneNote.OneNote.x-none.msi.16.x-none.xml	94.31 KB	d314151f6b60473f57e81f89e72009b02cfbcd4390e3048f736120e9383b48bc	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml	91.77 KB	ae39a4c092e5f81690c434d96d05ca28be0a1e6972798bada83b63393dc04d48	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPoint.PowerPoint.x-none.msi.16.x-none.xml	100.97 KB	0052ce84a95604fa41619e67a8bb307338dd4921d07efcb3ece2655e920b7dec	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.en-us.xml	25.47 KB	05a4da62d42e4498f015e35230c212978106f9cbe6526169f1a8c617fd92d75d	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.es-es.xml	24.53 KB	9f58f21d9cd5de9783b199767c3f2f277e69bcafd23fccc6fe763e87ca9e5be9	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.fr-fr.xml	24.53 KB	08567db5710d007f36a637f164f14df40959b9eafc65dd4fef49fa5f3055e16e	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Publisher.Publisher.x-none.msi.16.x-none.xml	75.97 KB	e102cfbd179dc7f4704b51fd27905a82c32517721e9fca03f6253edd131a1a62	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Word.Word.x-none.msi.16.x-none.xml	85.25 KB	32a73894c49e40b8443e5fcae640cafc2be2579030dfeaa48e0fb08fb8013619	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmui.msi.16.en-us.xml	56.69 KB	f18fe8ce4bb948d558dfa9a538f77faeb7914ce832f6452aca789535a2bb21c9	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmuiset.msi.16.en-us.xml	2.61 KB	be1d592cb3e97912c4337f1f4e5a8c1a57ccb4c5d236e4dc9be9ef9ff7ec3533	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.dcfmui.msi.16.en-us.xml	10.20 KB	5aea0f91d46c71615585f6eb808620e00209a58033fb66476d060c5c28633050	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.excelmui.msi.16.en-us.xml	34.82 KB	1a9c44b57285845814a0c999a4388729deb9af95833d13d9254e733a304d8098	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.groovemui.msi.16.en-us.xml	6.61 KB	39a25d43daaef81bc269a5535203028a55829434050363f0cf305fb31a6fbf1b	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.lyncmui.msi.16.en-us.xml	23.40 KB	59e96761e92ca77cb7d0a77e4bfef40242f2aaa1fefc40d119f603d4a321f433	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64muiset.msi.16.en-us.xml	2.61 KB	9ee8f1938caa96e62b5ca59e8d4330cf96daea26f91b0c6afc24dbdc72927949	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64ww.msi.16.x-none.xml	261.80 KB	45b7dcc8da7de7458b4aa6fdceec5022dff5e571fd7786a0eb40109385f495b5	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemui.msi.16.en-us.xml	104.99 KB	012255955dac349d2519ac5658544891d300c9ce5dad5335d3077f560906b5c6	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemuiset.msi.16.en-us.xml	2.61 KB	fe5a1bd5f89fca48ae85449e08455a0c3fc10ba19da1fc4dfeb98ab292eed926	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.onenotemui.msi.16.en-us.xml	19.14 KB	fe2d27ca22cf4cad0a8f0b2a1bfc9a9b5b371fd72ae4272c7be5a506a992a52a	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmmui.msi.16.en-us.xml	11.38 KB	59b1c677cd25252540420c6d0b246647d08bc0cd225d93d133795031b58a264a	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmuxmui.msi.16.en-us.xml	10.26 KB	b79fba62879f690247855352f10c292b815df5e12f0127742e2aa4f01b84c535	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.outlookmui.msi.16.en-us.xml	94.81 KB	c10419df976b15fa21d9dec87357e21bb4f5357330e0c2d953d524f0eaa9cdf8	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.powerpointmui.msi.16.en-us.xml	26.69 KB	9f2674be322ecb93fa07f0377b4195fdef5102b843b2b8d3b0555f2f34013702	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.proofing.msi.16.en-us.xml	2.61 KB	696f3342aa9157afc2dc91cc0054a1d88e99b154e62295521709ec7f873b5a90	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.publishermui.msi.16.en-us.xml	14.37 KB	b053880f5a75be12931499406b3f2cfa1ceda4af1038b330297c7897fd95ab5c	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.shared.Office.x-none.msi.16.x-none.xml	683.67 KB	5fc136dfc38d3db24559ad9f30a04b3873f7ef07f3de01892a8bcce4d8e7e621	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.wordmui.msi.16.en-us.xml	76.64 KB	7c0ea12db9e6431df4c29dea3284164c9f9a621f6c1b33c7314595561aa93531	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentFallBack2016.xml	3.85 KB	895f32c406aefd8e02f577fa7877e65cc19977fa70d8546168b734764882b02e	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentLogOn2016.xml	3.79 KB	4088697a52868a7a92c6d9b150d8177404f3eb5691ab723663cb16bb01b068f1	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe	840.22 KB	54dc6b8204b6ef806e7f24d262c236cd9dab26c47932d27d02ed38895e6d8eb8	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\msoutilstat.etw.man	110.65 KB	7a54b22464dba12e05a572d0b7c13117312dfd2f89e8bdae4bcad09470873794	✗
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man	624.08 KB	d3a728ac622b504b23c706854e1265515a70d59e52a3528958f6dac09eb28b6d	✗
C:\ProgramData\Microsoft\Crypto\SystemKeys\1fd8a841971dc8f18facf1d9475e3f87_03845cb8-7441-4a2f-8c0f-c90408af5778	2.14 KB	53ff745bb2b88fcdd94d4b10f34b5389a1a0b39957421b1b6813a45e225cf12f	✗
C:\ProgramData\Microsoft\Diagnosis\DownloadedScenarios\Windows.Uif.static	3.17 KB	d84bd0098e69b1be545b92f52cbc46f89b32b4f00de943e7f79f65908407e090	✗
C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json.bk	1.42 KB	05cae46c9c415d7c8b8f430057a48703801c52e15dc016043581aa978d452ced	✗
C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk	2.01 KB	591cbd8a103cf01414c4d19c35a3b257fb8db1028f358b925c509c3f18568908	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\IdentityCRL\INT\ppcrlconfig600.dll	24.33 KB	4893ba0508b5de748ba91da7662262d39f2f7219d62940b3622a2cbca228229a	✗
C:\ProgramData\Microsoft\IdentityCRL\production\ppcrlconfig600.dll	27.00 KB	70dab2535d4c92916598aa386a65b1dfa52edc49eea142e21e02f5575a35abc6	✗
C:\ProgramData\Microsoft\MF\Pending.GRL	15.24 KB	5af812305607d86d728355e50221d10df264c371fa0bd7a7f1bc0d2583f22547	✗
C:\ProgramData\Microsoft\MF\Active.GRL	15.24 KB	f675401b39801f817c8c2c81969a60b4b2ff4555f20f097ceec9ab062ac46f81	✗
C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\MasterDatastore.xml	901 bytes	b2f63dd2b3fbccccacb535ccaf6daf3bc61dbd080359b4b788b6f9abda096512	✗
C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\Power_0.provxml	2.39 KB	e65fc0e02f51e0b501b37e6056fe1ce0ffd61b24f7710822d4ca383827f6c707	✗
C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\Power_1.provxml	2.39 KB	5d64799d76bc3ed266c9408ee7078f04f0c85339c6b6267830d0ce2ce2f04a7a	✗
C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime.xml	1.16 KB	ca5b184336420878bab81fc1067b9f6a6361e5263a0f2023b4d802a0430cd48e	✗
C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\customizations.xml	4.26 KB	d05cc41287537692c7cfe0648a816c7f14edc394cdf019659c2dd03dbc541fc4	✗
C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\MasterDatastore.xml	901 bytes	7651a9251761b1c820471c51480040641b7fbed9d72692101d13ed810db19961	✗
C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime\Power_1.provxml	990 bytes	0c2d7f65ecd5c0571653090904ed546688446afd3378e9829a9a04e1967235f5	✗
C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime.xml	973 bytes	6a4146bbbb7f1de66881a59acf16114f57b559257c26dcac1cbe0a669c40df7d	✗
C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime\Power_0.provxml	990 bytes	f00863f6f3aed95206aff269d89098e7bb0bbdf324f4a852bde86697a9926205	✗
C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\customizations.xml	1.85 KB	369a0848402314cfc379b964483f9d17d2829afa20eec73876528016ff2f6be3	✗
C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\MasterDatastore.xml	901 bytes	31709c7a7ffc3b6d81e266950dddcc6bf98617b4328230b5fc148ffbb08a9aeb	✗
C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime\Power_0.provxml	3.83 KB	38050da36c1fb1e49f5b60739a0ba406922e40a66b907821d242e2463e8f4c3e	✗
C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime.xml	943 bytes	004726d80dfb8a74ee8cddce5c46192e27712e83c5c080d23843c8f244d70ed2	✗
C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime\Power_1.provxml	3.83 KB	dcc6f56792392d3ce43b8b0b6119e12bd832d63dcd21aa63be1a62766a367ca4	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\MasterDatastore.xml	901 bytes	5ff8576f395d1d1747849a74cef533cc33fdd2e06adde208dc6f745f919e0876	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_1.provxml	2.40 KB	86f55f36269783373392cbb773c7ce5c69faadb3fb860a8b16534b8a47629268	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_2.provxml	2.87 KB	f6c369bde748af81856f504824c747a3ae6421ceaca979173c3f4266779e07d9	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_0.provxml	3.58 KB	3a97ce3b293a1c4d51905cd683118e6a0437b2ac749c14123be282c8ff6b9e61	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime.xml	1.18 KB	799dcb5af6b8ad323591b82e8f478902df5bfcd620642ece7dc076b0da54d4d4	✗
C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\customizations.xml	7.00 KB	cd14d5f69c2de46bce3109817937633e2e517cfa4df67d6f811842f003c62eef	✗
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\MasterDatastore.xml	901 bytes	a58afb5152d2bc6ab76d1d0f35332ceef36fc3776192576b749598017c5d45c8	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime.xml	1.16 KB	fbb374d85d8912749eb1df93203e86a5530573eeeaa908e5259086a4332f23fc	✗
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_1.provxml	3.85 KB	c8ec4a69697671da1a9810d4eedc84ca93be44bf084759ac5205f769280eec77	✗
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_2.provxml	2.39 KB	24f98ad657794de2ee6fe1c1d741cc618b8fe0e88ed87496026b7c7521ef7b40	✗
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_0.provxml	4.56 KB	b75962decf1330571ddca24da5a8fcf44a2aaf02d01e478e05598a3be2cdbc76	✗
C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\customizations.xml	8.42 KB	825ce09e28d2caf9c883a1e1899b2c4ab27f20be2e02223da3c8934809c9c01f	✗
C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\MasterDatastore.xml	901 bytes	416ebd643791ebbb5881f06e6a47b6e122b3fa0af695f3454cb2692f02b2bb3a	✗
C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\RunTime\Power_0.provxml	1.14 KB	43f6036dcd3a71fca6822494380a490daa90dfcc4839beda1eaae4bfd5e886b1	✗
C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\RunTime.xml	833 bytes	34962dde4dd7322aca281fbba3547c22c0208d5086d53e40068465cb6548b2dd	✗
C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\customizations.xml	1.47 KB	b9ca64d8709f707e27123d136b70353d2d1866e7de5d2230ef1324cebd1d3319	✗
C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\MasterDatastore.xml	901 bytes	2eb7fb7425181d809ddd9fcd95118c7a2efef931f00f0c05669d5d21e59b9dca	✗
C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\Prov\RunTime\Power_0.provxml	2.22 KB	60b139270f626efed614ae24ff18b3c17eec4a07b630c234cafca7a9438ae665	✗
C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\customizations.xml	2.79 KB	b00683d06e716a7d08bfdc55b4a7cd1d2caed9f7f76ef4bf0cd0ec41fc73f571	✗
C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\Prov\RunTime.xml	978 bytes	9b17203b8ade47b2104e4e5ca21aa3f7f2dce8d220add5a5d04f3399f142f625	✗
C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\MasterDatastore.xml	901 bytes	148fdb0e89b99d5e7744fd62af79133e1d2b1b0fb9470d05d5321482b4ebe964	✗
C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\Prov\RunTime\Power_0.provxml	7.54 KB	7aed4b8823462028d994852e29e34d0ce4fd415110b9fa964c698c6e9b57fce1	✗
C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\Prov\RunTime.xml	978 bytes	4972134bd2add7e239ea9977691322ebe607e467b8b7d3a675eca5cd5ce71e00	✗
C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\customizations.xml	7.78 KB	29af08e1452cba2d21ff4d0a3b837cb3cb25afe4633ec1a2ef8178ecc0eccb97	✗
C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\MasterDatastore.xml	901 bytes	d6d1a3863229b7abc24afa44c51bac34a06ae0cd75ac4f21e3861d9127782729	✗
C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime\Power_1.provxml	2.38 KB	a9c8e607dbf6bbd4cc233e8bdf114667cbba5147c205912d48b6223826d24a8d	✗
C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime\Power_0.provxml	2.39 KB	8568d585f7f099bd6c1ec4cee32a07178d1528550fae722515856f3768f0ec18	✗
C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime.xml	943 bytes	e8919204e52e7e6c0f8e57eae8cdd9c0e5ff7b3dbcf881c9808767ea32674524	✗
C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\customizations.xml	3.89 KB	b2fbb4eb70d132772417622918273bd575003ed6b23792d257b4d39af5284830	✗
C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\Prov\RunTime\Power_0.provxml	2.21 KB	2c3bd3ea6939ba18307e31b3f1b5e2b7c98e8b6111ad0b3facd4b2b05ae6c656	✗
C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\Prov\RunTime.xml	978 bytes	fabf3aa13e2fcc08177ce589aed9eb881cfa4c156510d235641f31f581d905a8	✗
C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\MasterDatastore.xml	901 bytes	97f41d8b35adce8f987d2a098c8534e4d663ba1dcc9eee016c7e6ccb030efc5e	✗
C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\customizations.xml	2.77 KB	890ad9bad73302e4cb1b9e3b0eebb7185bbbca65215c0cbc819f1dff63ca8832	✗
C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\MasterDatastore.xml	901 bytes	c7029800d59b613a9ee5597ccab5c31fae02230df44c4baed9b818c904af8246	✗
C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\Prov\RunTime.xml	1.04 KB	d61c727f570c6afa2489efe95774cfb8c343265d99c37dff6253db29a7ace459	✗
C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\Prov\RunTime\Power_0.provxml	1.28 KB	65c6c85e07913162d1aff117607f8ff3e5c01e2173d80fb146592b7b3c9f03c2	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\customizations.xml	2.21 KB	0f160a8a46d50475d7f52e73e16ec500944c96834b2ccb9459de34a6c36c8be8	✗
C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\MasterDatastore.xml	901 bytes	68bd9ccef0d1244ca94cf0cc8fd6f8e4f4aa67c13cf75833d39a35d115785a4b	✗
C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\Prov\RunTime.xml	978 bytes	915ee5e67a1733dd73daf88dfb42768f39048a199d088bf00c06c1791c987784	✗
C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\MasterDatastore.xml	901 bytes	2b8befeb712d688a4cbe6d21ff774eeb7773210cdf6c3126f354aae9e25a049f	✗
C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime\Power_0.provxml	2.42 KB	079bfde0cfd8dd125520dea8429c8c430a940faf331343176a082c783b3a74b6	✗
C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime\Power_1.provxml	2.41 KB	97e612a8ae8ce293219d79a1bdb0f3e82eb797709199fc5619fa7d3e45ed3523	✗
C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime.xml	943 bytes	02a27f7aca9da7e58a9af1bdbb707b47396af744026eb264ca3e1d8a5d3bbe7a	✗
C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\customizations.xml	4.03 KB	53b7233ff20142ce0f3a93f9eab11eded7042a2a7527e8bce5a3b4aa22ce531a	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\MasterDatastore.xml	901 bytes	80485e8cc49a63a7073a79a50468ddd5d5e1c79bafe6252fde8805b82418b414	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_0.provxml	7.03 KB	2be2c67a8a1736aa0d58fa0d825a7299f06a7788441a5e1cdd959f4b5789965b	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_3.provxml	6.92 KB	10f335727e4c8f09407406086ca820c3f57c0b762ed0adc971afad06f545f8cf	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_1.provxml	2.00 KB	9a81feeec8c711740c45205b946b860757df3b827d879cfb0ac40aaa801bfcad	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_4.provxml	6.92 KB	fdc2dae2e991137dd5785b7078fe02a412300d7131db5ce1a194071c309dd390	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_2.provxml	4.64 KB	eb7fffdcf8c46eae537c6c9a0fdf950c07d27c2caf286489b3188d53e9a1e471	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_5.provxml	4.21 KB	8571d79dc8706cf20addf6afaf60955fc1e3d2bbc14fc5694cd530de601f7342	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_6.provxml	2.45 KB	53b722011b14da7440e08e94d2a3999f1b8475d45f15c4940b36160447574778	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_7.provxml	2.93 KB	590e61dbfb11704e787e95abc68639392bd3b89dbcd84855ed7849c5ebae40b4	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime.xml	2.07 KB	0f3c3aa48fe960f183619e5f678269782b0c3bd035b8e629c20de9dc3ff943bc	✗
C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\customizations.xml	28.29 KB	6620e3098b063d02f6e627d0b97c40592c6e7893564c2427b6398cd067766d0a	✗
C:\ProgramData\Microsoft\User Account Pictures\guest.bmp	588.67 KB	c543ce4a8a73e094a39f9aea16a604b1ca972a6a35fcbeacb3396dc40607d645	✗
C:\ProgramData\Microsoft\User Account Pictures\guest.png	5.89 KB	6d3080fda6cb3a2bc3cfe7115b170fd19c3a8e1bc40b0f7bfbaa62e724442c09	✗
C:\ProgramData\Microsoft\User Account Pictures\user-32.png	1.02 KB	3bb3064f088e346f5c7a0a4283a8165728e9ed1833927dde7985195ce2329c60	✗
C:\ProgramData\Microsoft\User Account Pictures\user-192.png	2.97 KB	2ffaabad027a37a0434f555a775c62cebc53152b793414f5d088c3b343cf6542	✗
C:\ProgramData\Microsoft\User Account Pictures\user-40.png	1.04 KB	7616f7f07fc9c6c2c3448b77aeb5e898e660af837558d3e9976dbcebb2637ad0	✗
C:\ProgramData\Microsoft\User Account Pictures\user-48.png	1.10 KB	8a960d09488b32548ba6727004b8cc2fab7dca9743c87cd00a7fc5d5d245e7e7	✗
C:\ProgramData\Microsoft\User Account Pictures\user.bmp	588.67 KB	a8dd5d6d705042105ff7a800c2ebcc34d3e72b8426580b391e79747a17f46689	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Microsoft\User Account Pictures\user.png	5.89 KB	7c12fe0fcc16c54bd859c208d4e539a3005955d33a6390332d63d192811d164d	✗
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\154E23D0-C644-4E6F-8CE6-5069272F999F.vsch	788 bytes	bae997787beb8098a7daedde557469aa7e51fe5a0380d9da04dae7226d037fd7	✗
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch	740 bytes	dc2570da3ae78321d2a02fd10878b28db5b5e3f0eccaef5f542b0732593cd92e	✗
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch	892 bytes	f5986e7330e084ffdce0aacedea6bedc88b6757dc9aab432c065e535929234fd	✗
C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol	1.05 KB	f1723d66b0bf3790cad9a446e931630580269b4d71a61fd925d747e5fcb84d27	✗
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\packages\vcRuntimeAdditional_x86\cab1.cab	5089.54 KB	35b51249f1134ff1631324081d3aef1bb0353ddbd395a7dbafce450d594de7c9	✗
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\packages\vcRuntimeAdditional_x86\vc_runtimeAdditional_x86.msi	180.62 KB	7d9c0ead1415aab02227953eee3eaba118379a19927aa68d220930f23972d2e1	✗
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab	974.30 KB	32a2404759b5511e0a00a1e4229bf8911dec37c380a78ccb27cd59b75e570fc2	✗
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x86\vc_runtimeMinimum_x86.msi	140.62 KB	2c104ed5c1234e849d341abdc3a00b28adc916cb7c42b58176154140d7fbf3b4	✗
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\packages\vcRuntimeMinimum_x86\cab1.cab	1336.23 KB	acf832846ba56b13391966cf498759814a1dc0049e7cbb35a1eaf599ecc9b0d3	✗
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\packages\vcRuntimeMinimum_x86\vc_runtimeMinimum_x86.msi	188.62 KB	7f7a92f396a439a0b6d08cfd0174fcec69691bc6bd3970a6bc76bbaf95cb5da1	✗

Reduced dataset

Host Behavior

Type	Count
Module	108
System	11
Environment	22
-	14
File	21307
-	110
Process	2

Network Behavior

Type	Count
HTTP	1
DNS	3
TCP	3

Process #2: cmd.exe

ID	2
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c ver
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131181, Reason: Child Process
Unmonitor End Time	End Time: 157001, Reason: Terminated
Monitor duration	25.82s
Return Code	0
PID	4180
Parent PID	1220
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	23
Environment	11
System	2

Process #4: cmd.exe

ID	4
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /C del C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 317415, Reason: Child Process
Unmonitor End Time	End Time: 319622, Reason: Terminated by Timeout
Monitor duration	2.21s
Return Code	Unknown
PID	4092
Parent PID	1220
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876	C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe	Sample File	1839.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
81b62a4a6aa5bdde76a1add523b018ccd69414a9c559e8a073eeaa9383545fed	C:\BOOTNXT, C:\\#_THIS_FILE_IS_ENCRYPTED_[4DDC4E26F3012C76]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	631 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
55100ff930a6edf6bbd1d3abb6f9f248d3b554f7c3824274b599c142cbf18cb2	C:\Boot\#_THIS_FILE_IS_ENCRYPTED_[99283AD8A3FE1DD2]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\Boot\BOOTSTAT.DAT	Modified File	64.62 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
01a67420abd3dc877f950b44abc31323259cbc8285b4e21910f24fdfb33ff5b4	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\MasterDescriptor.x-none.xml, C:\ProgramData\Mic... ...x-none.16\#_THIS_FILE_IS_ENCRYPTED_[CA0401F040336915]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	21.15 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
e8c2ece5a9e70556322dc6cc741422cfcd27be3394939deb38764e8f3b92e38c	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\#_THIS_FILE_IS_ENCRYPTED_[01759C4BB0F2879D]-[ID-... ...IL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\s321033.hash	Modified File	732 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
84b9b51439a6e62ae6786efce8b379405411be55f4bab3d59d81f1ec204bb879	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\#_THIS_FILE_IS_ENCRYPTED_[89F19639FD327258]-[ID-... ...rotonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\MasterDescriptor.en-us.xml	Modified File	22.46 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
b0de407bd3639b5310584a30f2f067a41e7ce6c9f0090787eb34ebf47534f61c	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\#_THIS_FILE_IS_ENCRYPTED_[CA5A36EA6886BA6C]-[ID-... ...@protonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\stream.x86.en-us.man.dat	Modified File	865.07 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
94e068068fa00f84f8f9b7f701a2682349bff9944ac4bfdd0b8830cf7b7e8bec	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\s320.hash, C:\ProgramData\Microsoft\ClickToRun\... ...x-none.16\#_THIS_FILE_IS_ENCRYPTED_[5A36FD5309D3E894]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	732 bytes	application/octet-stream	Create, Write, Access, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
42a934bee260294e880736d02f166c116247a1bbabcd8de2504234eafd5a7a42	C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\stream.x86.x-none.man.dat, C:\ProgramData\Micro... ...x-none.16\#_THIS_FILE_IS_ENCRYPTED_[DC72749AF4B85390]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	3630.07 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
0c88423b0e76dd3f192b08db9dbd104a7e2c9217d507ab883259be7aed02fe21	C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.2.xml, C:\ProgramData\Microsoft\ClickToRun\#_THIS_FILE_IS_ENCRYPTED_[D9D2359E62300C39]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.96 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7de3143aee32413b182d2865c787794cb8e53c855097f6136c3dce37e706a1a4	\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B1... ...ata\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserDeploymentConfiguration.xml	Modified File	1.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4e4bad77cdbb1e548548ce69fbbb8e513b8105d8682f9c9f6f14dfbd87572906	C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-6... ...163A08E8}\#_THIS_FILE_IS_ENCRYPTED_[244E9AE06B9A4EBB]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.21 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
ddfcd5ee896d4662e1822836e95c2094da0a649626a940c8aeeba6044e1bb3f8	C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.0.xml, C:\ProgramData\Microsoft\ClickToRun\#_THIS_FILE_IS_ENCRYPTED_[386AF2CB4C6D1CE7]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.54 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
782fd03b2cd8ef112d2a329c4e605c4b5342f4540684f832ad9c8b0167fd82fb	\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B1... ...ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\Manifest.xml	Modified File	4818.63 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a92291e624ef772551e097e2761beb3ec855d7894df088d982e002d4653bad25	\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B1... ...kToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserManifest.xml	Modified File	3024.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bd788b7af960f36237298194557e666cbb05f29ff721473aae0ad68bf921ed35	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[A4041C99F5201907]-[ID-9893949... ...EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\AirSpace.Etw.man	Modified File	276.15 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
23677d36bb54beac4a905aa7877f2f658c04df3f16724842348524e73ff46b88	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[43BF3552D1FC51D]-[ID-9893949...tan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Access.Access.x-none.msi.16.x-none.xml	Modified File	38.50 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bb768bfc920d1c19e769b3bb9a6bb38d0a3906024a5b7714383a24b236bf84b7	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[A3ED5AD951C89907]-[ID-9893949...om].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.DCF.DCF.x-none.msi.16.x-none.xml	Modified File	16.88 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
86a40103ab163cc37c27454f60311e9542df63a36cba7933864df384a64f9aaf	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[67F20CDA06872285]-[ID-9893949...satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Excel.Excel.x-none.msi.16.x-none.xml	Modified File	232.91 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0cd5011a8c03e69627a9cfaeb5dcdca63c9693794dbe2ca6cb0b88c8d2ce6196	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Groove.Groove.x-none.msi.16.x-none.xml	Modified File	36.37 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
d330bce45795685ab9f82c82695380b0d0bfa6370b86efe947698001c43d9f4a	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Lync.Lync.x-none.msi.16.x-none.xml, C:\Prog...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[EBDB6618A8E503D1]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	88.07 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a6df145ca8724e5c0d5fc01dba3ff774706fae60ac76520e684ada12f11adafc	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSM.OSM.x-none.msi.16.x-none.xml	Modified File	2.10 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
c4681417281899ca230de5269345bb499651c95ebe0621091a0136aa51a9fa58	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSMUX.OSMUX.x-none.msi.16.x-none.xml, C:\Pr...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[2933485261CFCDE1]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.86 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d314151f6b60473f57e81f89e72009b02cfbcd4390e3048f736120e9383b48bc	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OneNote.OneNote.x-none.msi.16.x-none.xml, C...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[A05837150218CE05]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	94.31 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ae39a4c092e5f81690c434d96d05ca28be0a1e6972798bada83b63393dc04d48	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[7999C75C2CD80B84]-[ID-9893949...n, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml	Modified File	91.77 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
f6a4f3db0a489a923d17b0e8533a36ad60cbeb4a2630e48fb10c1c72a80e31a9	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPivot.PowerPivot.x-none.msi.16.x-none.xml	Modified File	695.84 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
0052ce84a95604fa41619e67a8bb307338dd4921d07efcb3ece2655e920b7dec	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[16C7F6CE5AAB7AFD]-[ID-9893949...ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPoint.PowerPoint.x-none.msi.16.x-none.xml	Modified File	100.97 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
05a4da62d42e4498f015e35230c212978106f9cbe6526169f1a8c617fd92d75d	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.en-us.xml, C:\ProgramD... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[E76ECF273ED1CE3D]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	25.47 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9f58f21d9cd5de9783b199767c3f2f277e69bcafd23fccc6fe763e87ca9e5be9	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[63EA2297C7E8F809]-[ID-9893949....com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.es-es.xml	Modified File	24.53 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
08567db5710d007f36a637f164f14df40959b9eafc65dd4fef49fa5f3055e16e	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[B5175A7A13EB1F29]-[ID-9893949....com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.fr-fr.xml	Modified File	24.53 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e102cfbd179dc7f4704b51fd27905a82c32517721e9fca03f6253edd131a1a62	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Publisher.Publisher.x-none.msi.16.x-none.xm...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[58C92EF98AFC50F8]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	75.97 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
32a73894c49e40b8443e5fcae640cafc2be2579030dfeaa48e0fb08fb8013619	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[BE4632D17D91E644]-[ID-9893949....].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Word.Word.x-none.msi.16.x-none.xml	Modified File	85.25 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f18fe8ce4bb948d558dfa9a538f77faeb7914ce832f6452aca789535a2bb21c9	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmui.msi.16.en-us.xml, C:\ProgramData\...\...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[E118DE39692FA6FA]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	56.69 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
be1d592cb3e97912c4337f1f4e5a8c1a57ccb4c5d236e4dc9be9ef9ff7ec3533	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[57FB1A353023334C]-[ID-9893949...l.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmuiset.msi.16.en-us.xml	Modified File	2.61 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5aea0f91d46c71615585f6eb808620e00209a58033fb66476d060c5c28633050	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.dcfmui.msi.16.en-us.xml, C:\ProgramData\Mic...\...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[931C9A13B1CC37A5]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	10.20 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
1a9c44b57285845814a0c999a4388729deb9af95833d13d9254e733a304d8098	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[073B89FE46C8BA00]-[ID-9893949...\...nmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.excelmui.msi.16.en-us.xml	Modified File	34.82 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
39a25d43daaef81bc269a5535203028a55829434050363f0cf305fb31a6fbf1b	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[59A3D2D7018E4949]-[ID-9893949...\...mail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.groovemui.msi.16.en-us.xml	Modified File	6.61 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
59e96761e92ca77cb7d0a77e4bfef40242f2aaa1fefc40d119f603d4a321f433	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[8716DDF546293E39]-[ID-9893949...\...onmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.lyncmui.msi.16.en-us.xml	Modified File	23.40 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
876d451e9ec8c137100b1eb0b80ab6cf0ce9e1592498e29ecbcf24adb15cacbb	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64mui.msi.16.en-us.xml	Modified File	22.05 KB	application/octet-stream	Write, Access, Delete	CLEAN
9ee8f1938caa96e62b5ca59e8d4330cf96daea26f91b0c6afc24dbdc72927949	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[07E87E6189D6760D]-[ID-9893949...\...com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64muiset.msi.16.en-us.xml	Modified File	2.61 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
45b7dcc8da7de7458b4aa6fdceec5022dff5e571fd7786a0eb40109385f495b5	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[BB61665407031F13]-[ID-9893949... ...il.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64ww.msi.16.x-none.xml	Modified File	261.80 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
012255955dac349d2519ac5658544891d300c9ce5dad5335d3077f560906b5c6	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemui.msi.16.en-us.xml, C:\ProgramData\... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[B964149DD3765693]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	104.99 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
fe5a1bd5f89fca48ae85449e08455a0c3fc10ba19da1fc4dfeb98ab292eed926	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemuiset.msi.16.en-us.xml, C:\ProgramDa... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[8BBD4696EB0E8CC4]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.61 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
fe2d27ca22cf4cad0a8f0b2a1bfc9a9b5b371fd72ae4272c7be5a506a992a52a	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[B8A133BCB2B298C2]-[ID-9893949... ...ail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.onenotemui.msi.16.en-us.xml	Modified File	19.14 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
59b1c677cd25252540420c6d0b246647d08bc0cd225d93d133795031b58a264a	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmmui.msi.16.en-us.xml, C:\ProgramData\Mic... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[3A90074B6515A301]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	11.38 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b79fba62879f690247855352f10c292b815df5e12f0127742e2aa4f01b84c535	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[E51544CF19972E72]-[ID-9893949... ...nmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmuxmui.msi.16.en-us.xml	Modified File	10.26 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c10419df976b15fa21d9dec87357e21bb4f5357330e0c2d953d524f0eaa9cdf8	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.outlookmui.msi.16.en-us.xml, C:\ProgramData... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[F4744DEDFEB2216C]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	94.81 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
9f2674be322ecb93fa07f0377b4195fdef5102b843b2b8d3b0555f2f34013702	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.powerpointmui.msi.16.en-us.xml, C:\ProgramD... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[493282023081651A]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	26.69 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
696f3342aa9157afc2dc91cc0054a1d88e99b154e62295521709ec7f873b5a90	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.proofing.msi.16.en-us.xml, C:\ProgramData\M...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[825DB2012A7430A8]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.61 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b053880f5a75be12931499406b3f2cfa1ceda4af1038b330297c7897fd95ab5c	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[4B4A0953BA7E82D5]-[ID-9893949...l.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.publishermui.msi.16.en-us.xml	Modified File	14.37 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
5fc136dfc38d3db24559ad9f30a04b3873f7ef07f3de01892a8bcce4d8e7e621	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.shared.Office.x-none.msi.16.x-none.xml, C:\...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[A6CD167D9EB63600]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	683.67 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7c0ea12db9e6431df4c29dea3284164c9f9a621f6c1b33c7314595561aa93531	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[CD5611B6423A2B94]-[ID-9893949...onmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.wordmui.msi.16.en-us.xml	Modified File	76.64 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
895f32c406aefd8e02f577fa7877e65cc19977fa70d8546168b734764882b02e	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[34F2311A2FDE5C6A]-[ID-9893949... ..., C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentFallBack2016.xml	Modified File	3.85 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4088697a52868a7a92c6d9b150d8177404f3eb5691ab723663cb16bb01b068f1	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentLogOn2016.xml, C:\... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[A77C5FD0DBED5CA2]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	3.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
54dc6b8204b6ef806e7f24d262c236cd9dab26c47932d27d02ed38895e6d8eb8	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[DB5D92E6EE81E32A]-[ID-9893949... ...-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe	Modified File	840.22 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7a54b22464dba12e05a572d0b7c13117312dfd2f89e8bdae4bcad09470873794	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\msoutilstat.etw.man, C:\ProgramData\Microsoft\ClickToRu... ...B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[AD7687541F5C3F6C]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	110.65 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d3a728ac622b504b23c706854e1265515a70d59e52a3528958f6dac09eb28b6d	C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\#_THIS_FILE_IS_ENCRYPTED_[6941B3748A0B9B71]-[ID-9893949... ... 1F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\wordEtw.man	Modified File	624.08 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
d5673631655977454aa219208594cdbc6923a1275fe93ca4a978025693ee4869	C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\4eccd106f69e31c1b12304e5463bb71d_03845cb8-7441-4a2f-8c0f-c90408af5778	Modified File	686 bytes	application/octet-stream	Write, Access, Read, Delete	CLEAN
53ff745bb2b88fcdd94d4b10f34b5389a1a0b39957421b1b6813a45e225cf12f	C:\ProgramData\Microsoft\Crypto\SystemKeys\#_THIS_FILE_IS_ENCRYPTED_[C7E89F5379EE48DB]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAI... ...nmail.com].satan, C:\ProgramData\Microsoft\Crypto\SystemKeys\1fd8a841971dc8f18facf1d9475e3f87_03845cb8-7441-4a2f-8c0f-c90408af5778	Modified File	2.14 KB	application/octet-stream	Create, Write, Access, Delete	CLEAN
d84bd0098e69b1be545b92f52cbc46f89b32b4f00de943e7f79f65908407e090	C:\ProgramData\Microsoft\Diagnosis\DownloadedScenarios\#_THIS_FILE_IS_ENCRYPTED_[45DAE35AC80EF590]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Diagnosis\DownloadedScenarios\Windows.Uif.static	Modified File	3.17 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
05cae46c9c415d7c8b8f430057a48703801c52e15dc016043581aa978d452ced	C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json.bk, C:\ProgramData\Microsoft\Diagnosis\Dow... ...dSettings\#_THIS_FILE_IS_ENCRYPTED_[7E20F71967736CE9]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.42 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
591cbd8a103cf01414c4d19c35a3b257fb8db1028f358b925c509c3f18568908	C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\#_THIS_FILE_IS_ENCRYPTED_[4CB1EBA1218D1D66]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Diagnosis\DownloadedSettings\utc.app.json.bk	Modified File	2.01 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4893ba0508b5de748ba91da7662262d39f2f7219d62940b3622a2cbca228229a	C:\ProgramData\Microsoft\IdentityCRL\INT\#_THIS_FILE_IS_ENCRYPTED_[EFEA54BEAB010229]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\IdentityCRL\INT\ppcrlconfig600.dll	Modified File	24.33 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
70dab2535d4c92916598aa386a65b1dfa52edc49eea142e21e02f5575a35abc6	C:\ProgramData\Microsoft\IdentityCRL\production\#_THIS_FILE_IS_ENCRYPTED_[C16E72939346B7C2]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\IdentityCRL\production\ppcrlconfig600.dll	Modified File	27.00 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5af812305607d86d728355e50221d10df264c371fa0bd7a7f1bc0d2583f22547	C:\ProgramData\Microsoft\MF\Pending.GRL, C:\ProgramData\Microsoft\MF\#_THIS_FILE_IS_ENCRYPTED_[F888006D74602891]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	15.24 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f675401b39801f817c8c2c81969a60b4b2ff4555f20f097cec9ab062ac46f81	C:\ProgramData\Microsoft\MF\Active.GRL, C:\ProgramData\Microsoft\MF\#_THIS_FILE_IS_ENCRYPTED_[98FFE3AA4ED6BE06]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	15.24 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b2f63dd2b3fbccccacb535ccaf6daf3bc61dbd080359b4b788b6f9abda096512	C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi...\...fdbb8e49}\#_THIS_FILE_IS_ENCRYPTED_[2209A0125D034E1F]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e65fc0e02f51e0b501b37e6056fe1ce0ffd61b24f7710822d4ca383827f6c707	C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[D959BBD2FEF5D8...\...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\Power_0.provxml	Modified File	2.39 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5d64799d76bc3ed266c9408ee7078f04f0c85339c6b6267830d0ce2ce2f04a7a	C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[4EF15D820765AE...\...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime\Power_1.provxml	Modified File	2.39 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
ca5b184336420878bab81fc1067b9f6a6361e5263a0f2023b4d802a0430cd48e	C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\#_THIS_FILE_IS_ENCRYPTED_[ACEDA27F48730206]-[ID-...\...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\Prov\RunTime.xml	Modified File	1.16 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d05cc41287537692c7cfe0648a816c7f14edc394cdf019659c2dd03dbc541fc4	C:\ProgramData\Microsoft\Provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\customizations.xml, C:\ProgramData\Microsoft\Provisio...\...fdbb8e49}\#_THIS_FILE_IS_ENCRYPTED_[FD6C7F90C9B244CD]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	4.26 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7651a9251761b1c820471c51480040641b7fbed9d72692101d13ed810db19961	C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi... ...e341170f}\#_THIS_FILE_IS_ENCRYPTED_[B390714CB830659D]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0c2d7f65ecd5c0571653090904ed546688446afd3378e9829a9a04e1967235f5	C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime\Power_1.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[28AF6B31E47274C5]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	990 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6a4146bbbb7f1de66881a59acf16114f57b559257c26dcac1cbe0a669c40df7d	C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\#_THIS_FILE_IS_ENCRYPTED_[7B9DC3BF52422911]-[ID-... ...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime.xml	Modified File	973 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f00863f6f3aed95206aff269d89098e7bb0bbdf324f4a852bde86697a9926205	C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\Prov\RunTime\Power_0.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[B6058E5783504B72]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	990 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
369a0848402314cfc379b964483f9d17d2829afa20eec73876528016ff2f6be3	C:\ProgramData\Microsoft\Provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\customizations.xml, C:\ProgramData\Microsoft\Provisio... ...e341170f}\#_THIS_FILE_IS_ENCRYPTED_[98DC63BA1E5E8365]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.85 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
31709c7a7ffc3b6d81e266950dddcc6bf98617b4328230b5fc148ffbb08a9aeb	C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi... ...122a2271}\#_THIS_FILE_IS_ENCRYPTED_[8B796C224B1B65BD]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
38050da36c1fb1e49f5b60739a0ba406922e40a66b907821d242e2463e8f4c3e	C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime\Power_0.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[99E8F5D402F1218C]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	3.83 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
004726d80dfb8a74ee8cddce5c46192e27712e83c5c080d23843c8f244d70ed2	C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni... ...271}\Prov\#_THIS_FILE_IS_ENCRYPTED_[1A051E767A432201]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	943 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dcc6f56792392d3ce43b8b0b6119e12bd832d63dcd21aa63be1a62766a367ca4	C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[40C518819DD948...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\Prov\RunTime\Power_1.provxml	Modified File	3.83 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
ea98e3707398c0bc6ae10f09fcf2ea7ffa74e085c9935d19f128043d145f6632	C:\ProgramData\Microsoft\Provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\customizations.xml	Modified File	6.02 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
5ff8576f395d1d1747849a74cef533cc33fdd2e06adde208dc6f745f919e0876	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\#_THIS_FILE_IS_ENCRYPTED_[D814440E397413F3]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
86f55f36269783373392cbb773c7ce5c69faadb3fb860a8b16534b8a47629268	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_1.provxml, C:\ProgramData\Microsof...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[CABDE45CED7D0859]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.40 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f6c369bde748af81856f504824c747a3ae6421ceaca979173c3f4266779e07d9	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_2.provxml, C:\ProgramData\Microsof...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[1CAAEF61E7CA162B]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
3a97ce3b293a1c4d51905cd683118e6a0437b2ac749c14123be282c8ff6b9e61	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[0FF8D39C26151C...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime\Power_0.provxml	Modified File	3.58 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
799dcb5af6b8ad323591b82e8f478902df5bfcd620642ece7dc076b0da54d4d4	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni...48a}\Prov\#_THIS_FILE_IS_ENCRYPTED_[6E89216E8A2CA142]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.18 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
cd14d5f69c2de46bce3109817937633e2e517cfa4df67d6f811842f003c62eef	C:\ProgramData\Microsoft\Provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\customizations.xml, C:\ProgramData\Microsoft\Provisio... ...0f43548a}\#_THIS_FILE_IS_ENCRYPTED_[2952846CB8E67A8A]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	7.00 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a58afb5152d2bc6ab76d1d0f35332ceef36fc3776192576b749598017c5d45c8	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\#_THIS_FILE_IS_ENCRYPTED_[A681F748463CFDE7]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
fbb374d85d8912749eb1df93203e86a5530573eeeaa908e5259086a4332f23fc	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\#_THIS_FILE_IS_ENCRYPTED_[39CAD1A91C35198F]-[ID-... ...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime.xml	Modified File	1.16 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c8ec4a69697671da1a9810d4eedc84ca93be44bf084759ac5205f769280eec77	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[B5E5C315336820... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_1.provxml	Modified File	3.85 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
24f98ad657794de2ee6fe1c1d741cc618b8fe0e88ed87496026b7c7521ef7b40	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_2.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[3F4A8BD7E54A9530]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.39 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b75962decf1330571ddca24da5a8fcf44a2aaf02d01e478e05598a3be2cdbc76	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[FCF4DF08E12D92... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\Prov\RunTime\Power_0.provxml	Modified File	4.56 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
825ce09e28d2caf9c883a1e1899b2c4ab27f20be2e02223da3c8934809c9c01f	C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\#_THIS_FILE_IS_ENCRYPTED_[F6970239EF3A68CA]-[ID-98939... ...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\customizations.xml	Modified File	8.42 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
416ebd643791ebbb5881f06e6a47b6e122b3fa0af695f3454cb2692f02b2bb3a	C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi... ...817534df}\#_THIS_FILE_IS_ENCRYPTED_[2037D4335D0F46D7]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
43f6036dcd3a71fca6822494380a490daa90dfcc4839beda1eaae4bfd5e886b1	C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[31A02EEADB9403... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\RunTime\Power_0.provxml	Modified File	1.14 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
34962dde4dd7322aca281fbba3547c22c0208d5086d53e40068465cb6548b2dd	C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\#_THIS_FILE_IS_ENCRYPTED_[72FEEA7E21664A95]-[ID-... ...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\Prov\RunTime.xml	Modified File	833 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b9ca64d8709f707e27123d136b70353d2d1866e7de5d2230ef1324cebd1d3319	C:\ProgramData\Microsoft\Provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\customizations.xml, C:\ProgramData\Microsoft\Provisio... ...817534df}\#_THIS_FILE_IS_ENCRYPTED_[342C9555D8F818AB]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.47 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2eb7fb7425181d809ddd9fcd95118c7a2efef931f00f0c05669d5d21e59b9dca	C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\#_THIS_FILE_IS_ENCRYPTED_[E03FA1291AD439F6]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
60b139270f626efed614ae24ff18b3c17eec4a07b630c234cafca7a9438ae665	C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[E0EC5C21C31EBD... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\Prov\RunTime\Power_0.provxml	Modified File	2.22 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b00683d06e716a7d08bfdc55b4a7cd1d2caed9f7f76ef4bf0cd0ec41fc73f571	C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\customizations.xml, C:\ProgramData\Microsoft\Provisio... ...c8427b4e}\#_THIS_FILE_IS_ENCRYPTED_[238A8FB6E257506A]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9b17203b8ade47b2104e4e5ca21aa3f7f2dce8d220add5a5d04f3399f142f625	C:\ProgramData\Microsoft\Provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni... ...b4e}\Prov\#_THIS_FILE_IS_ENCRYPTED_[7206C490C3357C59]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	978 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
148fdb0e89b99d5e7744fd62af79133e1d2b1b0fb9470d05d5321482b4ebe964	C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\#_THIS_FILE_IS_ENCRYPTED_[63263BC4262DEDB0]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7aed4b8823462028d994852e29e34d0ce4fd415110b9fa964c698c6e9b57fce1	C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\Prov\RunTime\Power_0.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[CF08CE4BC45C39DD]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	7.54 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4972134bd2add7e239ea9977691322ebe607e467b8b7d3a675eca5cd5ce71e00	C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni... ...55e}\Prov\#_THIS_FILE_IS_ENCRYPTED_[BEC7C0011110DE24]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	978 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
29af08e1452cba2d21ff4d0a3b837cb3cb25afe4633ec1a2ef8178ecc0eccb97	C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\#_THIS_FILE_IS_ENCRYPTED_[00326E387944F92F]-[ID-98939... ...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\customizations.xml	Modified File	7.78 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d6d1a3863229b7abc24afa44c51bac34a06ae0cd75ac4f21e3861d9127782729	C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi... ...d2bfcfea}\#_THIS_FILE_IS_ENCRYPTED_[169B3B8CF2A64C5A]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a9c8e607dbf6bbd4cc233e8bdf114667cbba5147c205912d48b6223826d24a8d	C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime\Power_1.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[5C2EF1372C232590]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.38 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
8568d585f7f099bd6c1ec4cee32a07178d1528550fae722515856f3768f0ec18	C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[C3575DF87FB9EC... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime\Power_0.provxml	Modified File	2.39 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e8919204e52e7e6c0f8e57eae8cdd9c0e5ff7b3dbcf881c9808767ea32674524	C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni...\...fea}\Prov\#_THIS_FILE_IS_ENCRYPTED_[585AE829A3AD39BE]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	943 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b2fbb4eb70d1327724176229 18273bd575003ed6b23792d 257b4d39af5284830	C:\ProgramData\Microsoft\Provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\customizations.xml, C:\ProgramData\Microsoft\Provisio...\...d2bfcfea}\#_THIS_FILE_IS_ENCRYPTED_[A9D27D0BA2291083]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	3.89 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2c3bd3ea6939ba18307e31b 3f1b5e2b7c98e8b6111ad0b3 facd4b2b05ae6c656	C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[FAADE9B040C5E1... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\Prov\RunTime\Power_0.provxml	Modified File	2.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
fabf3aa13e2fcc08177ce589a ed9eb881cfa4c156510d2356 41f31f581d905a8	C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni...\...a09}\Prov\#_THIS_FILE_IS_ENCRYPTED_[EA83B6538714E342]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	978 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
97f41d8b35adce8f987d2a09 8c8534e4d663ba1dcc9eee0 16c7e6ccb030efc5e	C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi...\...d46f2a09}\#_THIS_FILE_IS_ENCRYPTED_[C2145F6BCF06C2D1]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
890ad9bad73302e4cb1b9e3 b0eebb7185bbbca65215c0c bc819f1dff63ca8832	C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\#_THIS_FILE_IS_ENCRYPTED_[684F989088C3B2CD]-[ID-98939... ...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\customizations.xml	Modified File	2.77 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c7029800d59b613a9ee5597 ccab5c31fae02230df44c4ba ed9b818c904af8246	C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi...\...d769311c}\#_THIS_FILE_IS_ENCRYPTED_[E531B94A16023A6D]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d61c727f570c6afa2489efe95 774cfb8c343265d99c37dff62 53db29a7ace459	C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni...\...11c}\Prov\#_THIS_FILE_IS_ENCRYPTED_[F9EF34A2968C1A01]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
65c6c85e07913162d1aff117607f8ff3e5c01e2173d80fb146592b7b3c9f03c2	C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\Prov\RunTime\Power_0.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[0BC6571FB80D535D]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.28 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0f160a8a46d50475d7f52e73e16ec500944c96834b2ccb9459de34a6c36c8be8	C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\#_THIS_FILE_IS_ENCRYPTED_[7CCD322E9112C470]-[ID-98939... ...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\customizations.xml	Modified File	2.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
68bd9ccef0d1244ca94cf0cc8fd6f8e4f4aa67c13cf75833d39a35d115785a4b	C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\#_THIS_FILE_IS_ENCRYPTED_[A02A2D3F09B59F05]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
915ee5e67a1733dd73daf88dfb42768f39048a199d088bf00c06c1791c987784	C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\Prov\#_THIS_FILE_IS_ENCRYPTED_[0E3573FB3AABFA23]-[ID-... ...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\Prov\RunTime.xml	Modified File	978 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
dc6da08d015ad48940540ed325b798689c620cbaf70f62fc366221a8be63b66d	C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\customizations.xml	Modified File	2.39 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
e1e2910d4b241c8a674e67e193f55908da64b690a687d976dd2287af6a30555a	C:\ProgramData\Microsoft\Provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\Prov\RunTime\Power_0.provxml	Modified File	1.64 KB	application/octet-stream	Write, Access, Read, Delete	CLEAN
2b8befeb712d688a4cbe6d21ff774eeb7773210cdf6c3126f354aae9e25a049f	C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\#_THIS_FILE_IS_ENCRYPTED_[44B30B2D549F86E3]-[ID-98939... ...-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\MasterDatastore.xml	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
079bfde0cfd8dd125520dea8429c8c430a940faf331343176a082c783b3a74b6	C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[9C335B53DFB25A... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime\Power_0.provxml	Modified File	2.42 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
97e612a8ae8ce293219d79a1bdb0f3e82eb797709199fc5619fa7d3e45ed3523	C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime\Power_1.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[C9CE1BC32AB661F0]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.41 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
02a27f7aca9da7e58a9af1bdbb707b47396af744026eb264ca3e1d8a5d3bbe7a	C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\#_THIS_FILE_IS_ENCRYPTED_[1B534C292614F555]-[ID-... ...AIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\Prov\RunTime.xml	Modified File	943 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
53b7233ff20142ce0f3a93f9eab11eded7042a2a7527e8bce5a3b4aa22ce531a	C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\#_THIS_FILE_IS_ENCRYPTED_[74BD0D99753C145E]-[ID-98939... ...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\customizations.xml	Modified File	4.03 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
80485e8cc49a63a7073a79a50468ddd5d5e1c79bafe6252fde8805b82418b414	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\MasterDatastore.xml, C:\ProgramData\Microsoft\Provisi... ...5fbedf62}\#_THIS_FILE_IS_ENCRYPTED_[0DE03F81BC02BCA8]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	901 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2be2c67a8a1736aa0d58fa0d825a7299f06a7788441a5e1cdd959f4b5789965b	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_0.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[5F9BC8669C756523]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	7.03 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
10f335727e4c8f0940740608 6ca820c3f57c0b762ed0adc971afad06f545f8cf	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_3.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[EA203CC84D717986]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	6.92 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9a81feeec8c711740c45205b946b860757df3b827d879cfb0ac40aaa801bfcad	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_1.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[E71FAF1058B98C1D]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.00 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
fdc2dae2e991137dd5785b7078fe02a412300d7131db5ce1a194071c309dd390	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_4.provxml, C:\ProgramData\Microsof... ...v\RunTime\#_THIS_FILE_IS_ENCRYPTED_[30CF3AD59E6A5F05]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	6.92 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
eb7fffdcf8c46eae537c6c9a0fdf950c07d27c2caf286489b3188d53e9a1e471	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\#_THIS_FILE_IS_ENCRYPTED_[B49E572B33D280... ...r@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_2.provxml	Modified File	4.64 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8571d79dc8706cf20addf6afaf60955fc1e3d2bbc14fc5694cd530de601f7342	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_5.provxml, C:\ProgramData\Microsof...\RunTime\#_THIS_FILE_IS_ENCRYPTED_[6B4269A89DC4E8C4]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	4.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
53b722011b14da7440e08e94d2a3999f1b8475d45f15c4940b36160447574778	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_6.provxml, C:\ProgramData\Microsof...\RunTime\#_THIS_FILE_IS_ENCRYPTED_[70F3E5048D1CF6B5]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.45 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
590e61dbfb11704e787e95abc68639392bd3b89dbcd848535ed7849c5ebae40b4	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime\Power_7.provxml, C:\ProgramData\Microsof...\RunTime\#_THIS_FILE_IS_ENCRYPTED_[99FB2980437485AD]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.93 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0f3c3aa48fe960f183619e5f678269782b0c3bd035b8e629c20de9dc3ff943bc	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\Prov\RunTime.xml, C:\ProgramData\Microsoft\Provisioni...f62}\Prov\#_THIS_FILE_IS_ENCRYPTED_[1AECF2C8878FAFC5]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	2.07 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6620e3098b063d02f6e627d0b97c40592c6e7893564c2427b6398cd067766d0a	C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\#_THIS_FILE_IS_ENCRYPTED_[B55F0558CEFEC13C]-[ID-98939...L-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Provisioning\{fc01e91f-914c-45af-9d7c-0b2e5fbedf62}\customizations.xml	Modified File	28.29 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c543ce4a8a73e094a39f9aea16a604b1ca972a6a35fcbeacb3396dc40607d645	C:\ProgramData\Microsoft\User Account Pictures\guest.bmp, C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[DC9762122EB5C383]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	588.67 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6d3080fda6cb3a2bc3cfe7115b170fd19c3a8e1bc40b0f7bfbaa62e724442c09	C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[F7538BA494DE3719]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\User Account Pictures\guest.png	Modified File	5.89 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
3bb3064f088e346f5c7a0a4283a8165728e9ed1833927dde7985195ce2329c60	C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[5B071F83C9887E8B]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\User Account Pictures\user-32.png	Modified File	1.02 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2ffaabad027a37a0434f555a775c62cebc53152b793414f5d088c3b343cf6542	C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[0755F82E35FD798E]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\User Account Pictures\user-192.png	Modified File	2.97 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7616f7f07fc9c6c2c3448b77aeb5e898e660af837558d3e9976dbcebb2637ad0	C:\ProgramData\Microsoft\User Account Pictures\user-40.png, C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[E8F0A05603BAC944]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
8a960d09488b32548ba6727004b8cc2fab7dca9743c87cd00a7fc5d5d245e7e7	C:\ProgramData\Microsoft\User Account Pictures\user-48.png, C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[AAD4492FAC4DAC28]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	1.10 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a8dd5d6d705042105ff7a800c2ebcc34d3e72b8426580b391e79747a17f46689	C:\ProgramData\Microsoft\User Account Pictures\user.bmp, C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[9D8FD99F18F6AAC9]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	588.67 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7c12fe0fcc16c54bd859c208d4e539a3005955d33a6390332d63d192811d164d	C:\ProgramData\Microsoft\User Account Pictures\user.png, C:\ProgramData\Microsoft\User Account Pictures\#_THIS_FILE_IS_ENCRYPTED_[ACE5F7AF9F76BD7C]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	5.89 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bae997787beb8098a7daedde557469aa7e51fe5a0380d9da04dae7226d037fd7	C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\#_THIS_FILE_IS_ENCRYPTED_[888FB0D55BEDC80]-[ID-9893949947FDA5... ...otonmail.com].satan, C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\154E23D0-C644-4E6F-8CE6-5069272F999F.vsch	Modified File	788 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
dc2570da3ae78321d2a02fd10878b28db5b5e3f0eccaef5f542b0732593cd92e	C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch, C:\ProgramData\Micr... ...EDAB3F204\#_THIS_FILE_IS_ENCRYPTED_[44BE36966166B9B4]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	740 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f5986e7330e084ffdce0aaceda6bedc88b6757dc9aab432c065e535929234fd	C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch, C:\ProgramData\Micr... ...EDAB3F204\#_THIS_FILE_IS_ENCRYPTED_[9DC305D35B50F53F]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	892 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f1723d66b0bf3790cad9a446e931630580269b4d71a61fd925d747e5fcb84d27	C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\#_THIS_FILE_IS_ENCRYPTED_[413639F86FB8C36F]-[ID-9893949947FDA5... ... 30B74801F]-[EMAIL-MREncptor@protonmail.com].satan, C:\ProgramData\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol	Modified File	1.05 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Windows\Temp\satan\	Accessed File	Create, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\Temp\satan\satan0	Dropped File	Create, Write, Access, Read	CLEAN
C:\Windows\Temp\satan\satan1	Dropped File	Create, Write, Access, Read	CLEAN
share.txt	Accessed File	Access	CLEAN
A:\	Accessed File	Access	CLEAN
B:\	Accessed File	Access	CLEAN
C:\	Accessed File	Access	CLEAN
D:\	Accessed File	Access	CLEAN
E:\	Accessed File	Access	CLEAN
F:\	Accessed File	Access	CLEAN
G:\	Accessed File	Access	CLEAN
H:\	Accessed File	Access	CLEAN
I:\	Accessed File	Access	CLEAN
J:\	Accessed File	Access	CLEAN
K:\	Accessed File	Access	CLEAN
L:\	Accessed File	Access	CLEAN
M:\	Accessed File	Access	CLEAN
N:\	Accessed File	Access	CLEAN
O:\	Accessed File	Access	CLEAN
P:\	Accessed File	Access	CLEAN
Q:\	Accessed File	Access	CLEAN
R:\	Accessed File	Access	CLEAN
S:\	Accessed File	Access	CLEAN
T:\	Accessed File	Access	CLEAN
U:\	Accessed File	Access	CLEAN
V:\	Accessed File	Access	CLEAN
W:\	Accessed File	Access	CLEAN
X:\	Accessed File	Access	CLEAN
Y:\	Accessed File	Access	CLEAN
Z:\	Accessed File	Access	CLEAN
C\# SATAN CRYPTOR #.hta	Accessed File	Access	CLEAN
C:\\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\$Recycle.Bin	Accessed File	Access	CLEAN
C:\BOOTNXT	Modified File	Write, Access, Read, Delete	CLEAN
C:\BOOTSECT.BAK	Accessed File	Access	CLEAN
C:\Boot	Accessed File	Access	CLEAN
C:\Boot\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\BCD	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG	Accessed File	Access	CLEAN
C:\Boot\BCD.LOG1	Accessed File	Access, Read	CLEAN
C:\Boot\BCD.LOG2	Accessed File	Access, Read	CLEAN
C:\Boot\BOOTSTAT.DAT	Modified File	Write, Access, Read, Delete	CLEAN
C:\Boot\Fonts	Accessed File	Access	CLEAN
C:\\#_THIS_FILE_IS_ENCRYPTED_[4DDC4E26F3012C76]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	Create, Write, Access	CLEAN
C:\Boot\Fonts\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\Fonts\chs_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\cht_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\jpn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\kor_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\malgun_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\malgunn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\meiryo_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\meiryon_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msjh_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\#_THIS_FILE_IS_ENCRYPTED_[99283AD8A3FE1DD2]-[ID-9893949947FDA5A23D8DE0930B74801F]-[EMAIL-MREncptor@protonmail.com].satan	Modified File	Create, Write, Access	CLEAN
C:\Boot\Fonts\msjhn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msyh_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\msyhn_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segmono_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segoe_slboot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\segoen_slboot.ttf	Accessed File	Access	CLEAN
C:\Boot\Fonts\wgl4_boot.ttf	Accessed File	Access	CLEAN
C:\Boot\Resources	Accessed File	Access	CLEAN
C:\Boot\Resources\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\Resources\bootres.dll	Accessed File	Access	CLEAN
C:\Boot\Resources\en-US	Accessed File	Access	CLEAN
C:\Boot\Resources\en-US\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\Resources\en-US\bootres.dll.mui	Accessed File	Access	CLEAN
C:\Boot\bg-BG	Accessed File	Access	CLEAN
C:\Boot\bg-BG\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\bg-BG\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\bootvhd.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\cs-CZ	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\cs-CZ\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\da-DK	Accessed File	Access	CLEAN
C:\Boot\da-DK\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\da-DK\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\da-DK\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\de-DE	Accessed File	Access	CLEAN
C:\Boot\de-DE\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
cmd.com	Accessed File	Access	CLEAN
cmd.exe	Accessed File	Access	CLEAN
cmd.bat	Accessed File	Access	CLEAN
cmd.cmd	Accessed File	Access	CLEAN
cmd.vbs	Accessed File	Access	CLEAN
cmd.vbe	Accessed File	Access	CLEAN
cmd.js	Accessed File	Access	CLEAN
cmd.jse	Accessed File	Access	CLEAN
cmd.wsf	Accessed File	Access	CLEAN
cmd.wsh	Accessed File	Access	CLEAN
cmd.msc	Accessed File	Access	CLEAN
C:\Windows\system32\cmd.com	Accessed File	Access	CLEAN
C:\Windows\system32\cmd.exe	Accessed File	Access	CLEAN
NUL	Accessed File	Access	CLEAN
C:\Boot\de-DE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\de-DE\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\el-GR	Accessed File	Access	CLEAN
C:\Boot\el-GR\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\el-GR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\el-GR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-GB	Accessed File	Access	CLEAN
C:\Boot\en-GB\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\en-GB\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\en-US	Accessed File	Access	CLEAN
C:\Boot\en-US\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\en-US\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\en-US\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-ES	Accessed File	Access	CLEAN
C:\Boot\es-ES\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\es-ES\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-ES\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\es-MX	Accessed File	Access	CLEAN
C:\Boot\es-MX\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\es-MX\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\et-EE	Accessed File	Access	CLEAN
C:\Boot\et-EE\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\et-EE\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fi-FI	Accessed File	Access	CLEAN
C:\Boot\fi-FI\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\fi-FI\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fi-FI\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-CA	Accessed File	Access	CLEAN
C:\Boot\fr-CA\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\fr-CA\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-FR	Accessed File	Access	CLEAN
C:\Boot\fr-FR\# SATAN CRYPTOR #.hta	Dropped File	Create, Access	CLEAN
C:\Boot\fr-FR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\fr-FR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hr-HR	Accessed File	Access	CLEAN
C:\Boot\hr-HR\# SATAN CRYPTOR #.hta	Dropped File	Create, Access	CLEAN
C:\Boot\hr-HR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hu-HU	Accessed File	Access	CLEAN
C:\Boot\hu-HU\# SATAN CRYPTOR #.hta	Dropped File	Create, Access	CLEAN
C:\Boot\hu-HU\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\hu-HU\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\it-IT	Accessed File	Access	CLEAN
C:\Boot\it-IT\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\it-IT\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\it-IT\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ja-JP	Accessed File	Access	CLEAN
C:\Boot\ja-JP\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\ja-JP\bootmgr.exe.mui	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\ja-JP\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ko-KR	Accessed File	Access	CLEAN
C:\Boot\ko-KR\# SATAN CRYPTOR #.hta	Dropped File	Create, Write, Access	CLEAN
C:\Boot\ko-KR\bootmgr.exe.mui	Accessed File	Access	CLEAN
C:\Boot\ko-KR\memtest.exe.mui	Accessed File	Access	CLEAN
C:\Boot\lt-LT	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://extreme-ip-lookup.com/json/	-	37.48.65.182	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	149.154.167.220	-	DNS	CLEAN
extreme-ip-lookup.com	109.236.91.3, 37.48.65.182	-	HTTP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
192.168.0.1	-	-	UDP, DNS	CLEAN
37.48.65.182	extreme-ip-lookup.com	Netherlands	TCP, HTTP, DNS	CLEAN
149.154.167.220	api.telegram.org	United Kingdom	TCP, DNS, TLS	CLEAN
109.236.91.3	extreme-ip-lookup.com	Netherlands	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	access, read	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	access, read	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	access, read	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c566662876.exe	"C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe"	MALICIOUS
cmd.exe	cmd /c ver	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /C del C:\Users\RDhJ0CNFevzX\Desktop\dd286a4d79d0f4c2b906073c7f46680252ca09c1c39b0dc12c92097c56662876.exe	CLEAN

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

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