ID: 572441
Sample Name:
evilnominatuscrypto
Cookbook: default.jbs
Time: 10:00:59
Date: 15/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

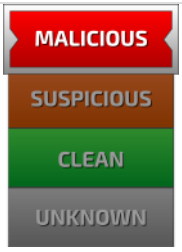
evilnominatuscrypto

Overview

General Information

Sample Name:	evilnominatuscrypto (renamed file extension from none to exe)
Analysis ID:	572441
MD5:	7cdf50ee4f3d0fe..
SHA1:	0170c2deae4486..
SHA256:	69811a6c9376b2..
Tags:	evilnominatuscrypto, exe, filecoder, msil, ransomware, screenlocker
Infos:	

Detection



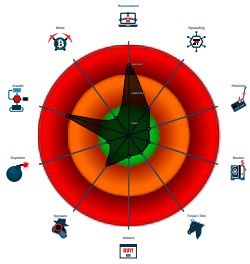
Voidcrypt

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: Shadow Copies De…
- Yara detected Voidcrypt Ransomwa…
- Sigma detected: Copying Sensitive …
- Creates files in the recycle bin to hid…
- Obfuscated command line found
- Deletes shadow drive data (may be …
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- evilnominatuscrypto.exe (PID: 6516 cmdline: "C:\Users\user\Desktop\evilnominatuscrypto.exe" MD5: 7CDF50EE4F3D0FEBC70DD36298ED07DA)
  - cmd.exe (PID: 6832 cmdline: "C:\Windows\System32\cmd.exe" /C echo ^[autorun^] >autorun.inf MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6956 cmdline: "C:\Windows\System32\cmd.exe" /C echo ^open^=KasperskyScan^.exe >>autorun.inf MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7004 cmdline: "C:\Windows\System32\cmd.exe" /C echo ^execute=^KasperskyScan^.exe >>autorun.inf MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 7052 cmdline: "C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet && wmic shadowcopy delete MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - vssadmin.exe (PID: 7092 cmdline: vssadmin delete shadows /all /quiet MD5: 7E30B94672107D3381A1D175CF18C147)
- OpenWith.exe (PID: 5772 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: D179D03728E95E040A889F760C1FC402)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
evilnominatuscrypto.exe	Destructive_Ransomware_Gen1	Detects destructive malware	Florian Roth	• 0x492a:$x2: delete shadows /all /quiet

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.880899143.0000000002421000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Voidcrypt	Yara detected Voidcrypt Ransomware	Joe Security	
Process Memory Space: evilnominatuscrypto.exe PID: 6516	JoeSecurity_Voidcrypt	Yara detected Voidcrypt Ransomware	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.evilnominatuscrypto.exe.170000.0.unpack	Destructive_Ransomware_Gen1	Detects destructive malware	Florian Roth	• 0x492a:$x2: delete shadows /all /quiet
1.0.evilnominatuscrypto.exe.170000.0.unpack	Destructive_Ransomware_Gen1	Detects destructive malware	Florian Roth	• 0x492a:$x2: delete shadows /all /quiet

Sigma Signatures

System Summary

Sigma detected: Shadow Copies Deletion Using Operating Systems Utilities

Sigma detected: Copying Sensitive Files with Credential Data

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Spam, unwanted Advertisements and Ransom Demands

Yara detected Voidcrypt Ransomware

Deletes shadow drive data (may be related to ransomware)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection

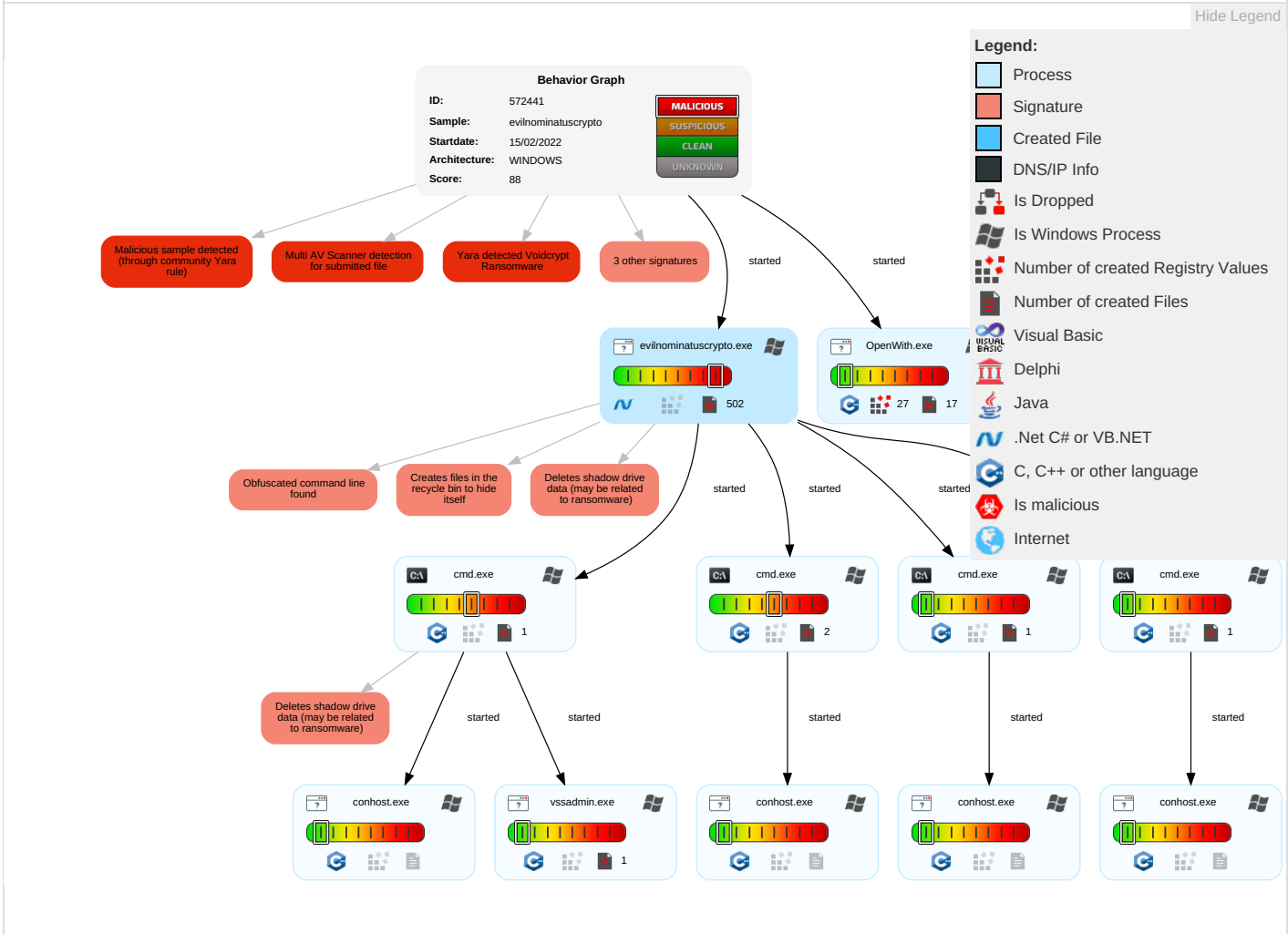
Creates files in the recycle bin to hide itself

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 File Deletion	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

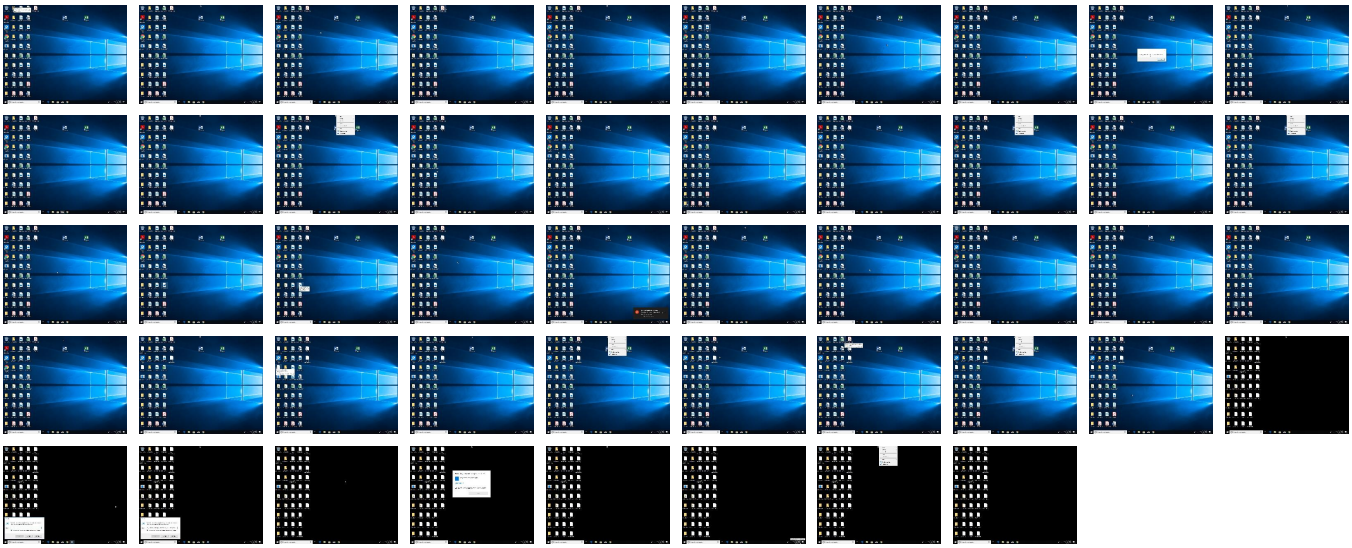
Behavior Graph

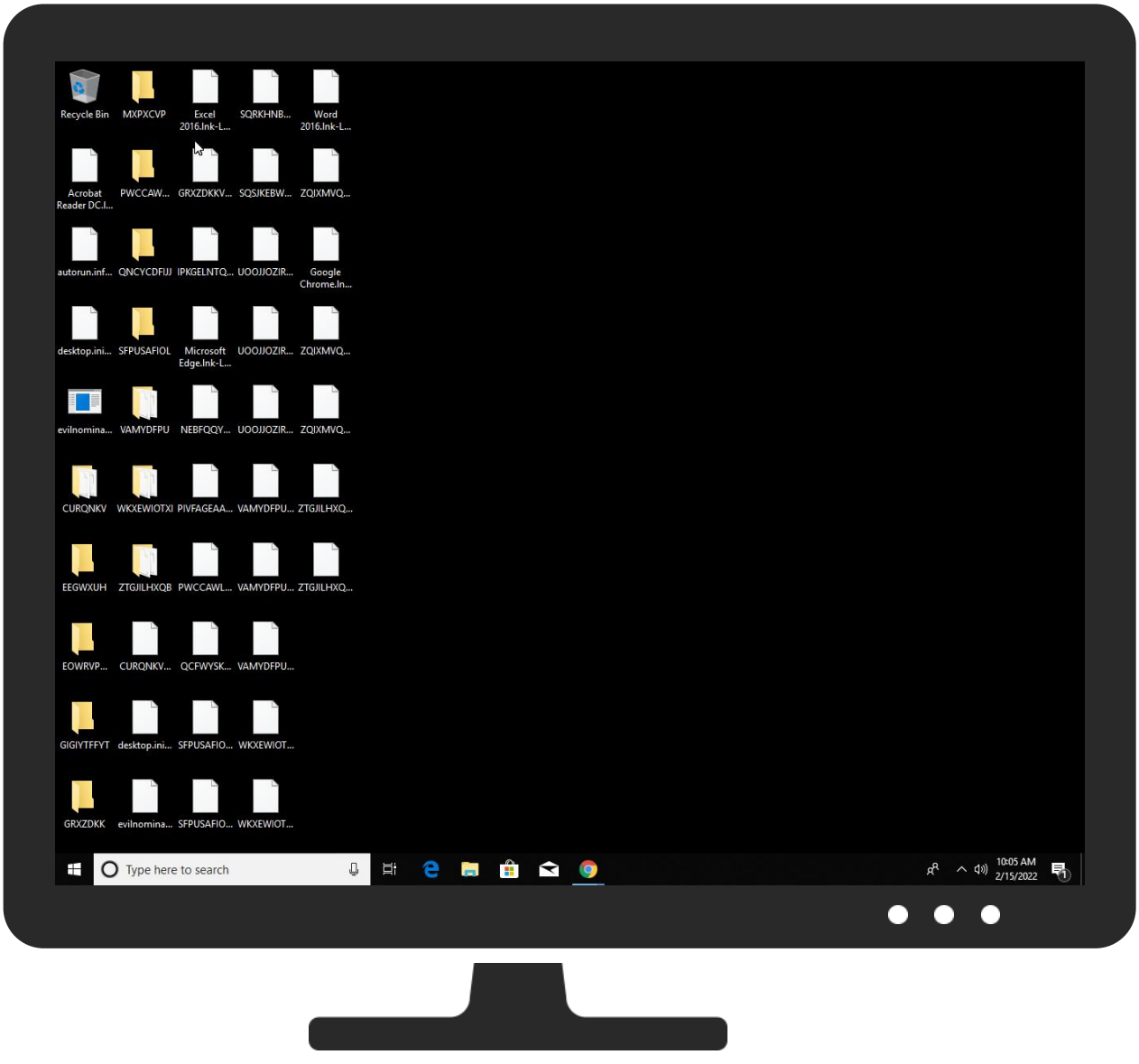


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
evilnominatuscrypto.exe	51%	Virustotal		Browse
evilnominatuscrypto.exe	29%	Metadefender		Browse
evilnominatuscrypto.exe	44%	ReversingLabs	ByteCode-MSIL.Ransomware.WannaCry	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com8	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	URL Reputation	safe	
http://www.fontbureau.comld	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krim	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-%	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/_$	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com8	evilnominatuscrypto.exe, 00000001.00000003.358343551.00000000053B5000.00000004.00000800.00020000.00000000.sdmp, evilnominatuscrypto.exe, 00000001.00000003.358456672.00000000053B6000.00000004.00000800.00020000.00000000.sdmp, evilnominatuscrypto.exe, 00000001.00000003.358185463.00000000053B5000.00000004.00000800.00020000.00000000.sdmp, evilnominatuscrypto.exe, 00000001.00000003.358058935.00000000053B6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	evilnominatuscrypto.exe, 00000001.00000003.358287424.000000000539A000.00000004.00000800.00020000.00000000.sdmp, evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	evilnominatuscrypto.exe, 00000001.00000002.892987211.0000000006592000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnva	evilnominatuscrypto.exe, 00000001.00000003.358651789.000000000539A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comld	evilnominatuscrypto.exe, 00000001.00000002.892448776.0000000005380000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	evilnominatuscrypto.exe, 00000001.00000002.892448776.0000000005380000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	evilnominatuscrypto.exe, 00000001.000000 02.892987211.0000000006592000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krim	evilnominatuscrypto.exe, 00000001.000000 03.356657263.0000000005394000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	evilnominatuscrypto.exe, 00000001.000000 02.892987211.0000000006592000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	evilnominatuscrypto.exe, 00000001.000000 02.892987211.0000000006592000.00000004.0 0000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comv	evilnominatuscrypto.exe, 00000001.000000 02.892448776.0000000005380000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	evilnominatuscrypto.exe, 00000001.000000 02.892987211.0000000006592000.00000004.0 0000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn-%	evilnominatuscrypto.exe, 00000001.000000 03.358651789.000000000539A000.00000004.0 0000800.00020000.00000000.sdmp, evilnomi natuscrypto.exe, 00000001.00000003.35811 3326.0000000005395000.00000004.00000800. 00020000.00000000.sdmp, evilnominatuscrypto.exe, 0 0000001.00000003.357784973.0000000005395 000.00000004.00000800.00020000.00000000.sdmp, evilnominatuscrypto.exe, 00000001.00000003.3 57597980.0000000005392000.00000004.00000 800.00020000.00000000.sdmp, evilnominatu scrypto.exe, 00000001.00000003.358231059 .0000000005396000.00000004.00000800.0002 0000.00000000.sdmp, evilnominatuscrypto.exe, 00000 001.00000003.358287424.000000000539A000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/_$	evilnominatuscrypto.exe, 00000001.000000 03.358113326.0000000005395000.00000004.0 0000800.00020000.00000000.sdmp, evilnomi natuscrypto.exe, 00000001.00000003.35778 4973.0000000005395000.00000004.00000800. 00020000.00000000.sdmp, evilnominatuscrypto.exe, 0 0000001.00000003.357597980.0000000005392 000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	evilnominatuscrypto.exe, 00000001.000000 03.356657263.0000000005394000.00000004.0 0000800.00020000.00000000.sdmp, evilnomi natuscrypto.exe, 00000001.00000002.89298 7211.0000000006592000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	evilnominatuscrypto.exe, 00000001.000000 02.892987211.0000000006592000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	evilnominatuscrypto.exe, 00000001.000000 03.358651789.000000000539A000.00000004.0 0000800.00020000.00000000.sdmp, evilnomi natuscrypto.exe, 00000001.00000002.89298 7211.0000000006592000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	evilnominatuscrypto.exe, 00000001.000000 03.361520866.000000000538D000.00000004.0 0000800.00020000.00000000.sdmp, evilnomi natuscrypto.exe, 00000001.00000002.89298 7211.0000000006592000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	572441
Start date:	15.02.2022
Start time:	10:00:59

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	evilnominatuscrypto (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.rans.evad.winEXE@16/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 56% • Quality standard deviation: 39.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, dllhost.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, VSSVC.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target evilnominatuscrypto.exe, PID 6516 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:05:25	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini-Locked
10:05:35	API Interceptor	1x Sleep call for process: OpenWith.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\ThumbCacheToDelete\thm6B05.tmp (copy)

Process:	C:\Windows\System32\OpenWith.exe
File Type:	data
Category:	dropped
Size (bytes):	7416
Entropy (8bit):	0.020297149862451055
Encrypted:	false
SSDEEP:	3:tn1lllF:y
MD5:	B710BC2FE0046515794A3E2977E9A15E
SHA1:	833EF452338434B5EB757F488DC7E993F9391C82
SHA-256:	2B79AF0DD12B22F34483108837981FBBADBB604367FCDA8B0A41807E8049A62E
SHA-512:	33C446E80358AFDACE96A393E13B5A76FDE58B7D60B17FF74FD6B2E8D1C69C685C9893295D57376F57D4BA4DFF2824DED5D23638CB26A160AAA4A429557E003
Malicious:	false
Reputation:	low
Preview:	..0 IMMM .....e..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db

Process:	C:\Windows\System32\OpenWith.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.408222675578688
Encrypted:	false
SSDEEP:	3:d:d
MD5:	419A089E66B9E18ADA06C459B000CB4D
SHA1:	ED2108A58BA73AC18C3D2BF0D8C1890C2632B05A
SHA-256:	C48E42E9AB4E25B92C43A7B0416D463B9FF7C69541E4623A39513BC98085F424
SHA-512:	BBD57BEA7159748E1B13B3E459E2C8691A46BDC9323AFDB9DBF9D8F09511750D46A1D98C717C7ADCA07D79EDC859E925476DD03231507F37F45775C0A79A59C
Malicious:	false
Preview:	CMMM .....

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db

Process:	C:\Windows\System32\OpenWith.exe
File Type:	data

Category:	dropped
Size (bytes):	7416
Entropy (8bit):	0.020297149862451055
Encrypted:	false
SSDEEP:	3:tn1lIlF:y
MD5:	B710BC2FE0046515794A3E2977E9A15E
SHA1:	833EF452338434B5EB757F488DC7E993F9391C82
SHA-256:	2B79AF0DD12B22F34483108837981FBBADBB604367FCDA8B0A41807E8049A62E
SHA-512:	33C446E80358AFDACE96A393E13B5A76FDE58B7D60B17FF74FD6B2E8D1C69C685C9893295D57376F57D4BA4DFF2824DED5D23638CB26A160AAA4A429557E003
Malicious:	false
Preview:	..0 IMMM .....e..... ....

C:\Users\user\Desktop\autorun.inf

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	65
Entropy (8bit):	4.255167483172791
Encrypted:	false
SSDEEP:	3:ltl6dFOcNt1HjWVFOcNtv:eIG1KVFv
MD5:	FBEFA88E6B51C05DD63D97DFDBEB3589
SHA1:	67E09918D878C6615BEFAB5DC9194439027F268D
SHA-256:	3861ACEDFFD29452D2FDB96728F7347652BDE9353915D3873A7414843F49B8B1
SHA-512:	58F8C1A64F2EB21BE7B96DB335D1ADE0CE0878566A8386B3689B650132CA28E14761B20FDFE50F2AF9915DFF2BDD3A5B07F6F3ED082E4E6998EC5F0CD052F1F
Malicious:	false
Preview:	[autorun] ..open=KasperskyScan.exe ..execute=KasperskyScan.exe ..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.218587302420799
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	evilnominatuscrypto.exe
File size:	32768
MD5:	7cdf50ee4f3d0febc70dd36298ed07da
SHA1:	0170c2deae4486a43894c202ea92d43556218e1c
SHA256:	69811a6c9376b219b335a055cfa970d38cd768abeca7138a2c1905560d468fef
SHA512:	370023f24390173044b2b32546b5ff68bc8786edfcd8784d0adfb9cede550d40a744df184303ccd16f277595d319671445e5f1c070f0e453d1b94b1dc70d7a28
SSDEEP:	384:AjdXpgpMf76oJgkB4nokwFwA4Ep/0VUx/Nx9DPxmB++6iCjGnLBs0Rr:adZgpCOagkBRp/0ut9Y++6iCjs2wr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<..b.....P... .....>i... ....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x693e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x0
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x6209133C [Sun Feb 13 14:18:36 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00002000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x68ec	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x820	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x67b4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x4944	0x5000	False	0.504150390625	data	5.53179387013	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x820	0x1000	False	0.229248046875	data	3.05099161152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x1000	False	0.0087890625	data	0.0131269437212	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x80a0	0x2ec	data		
RT_MANIFEST	0x8390	0x489	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

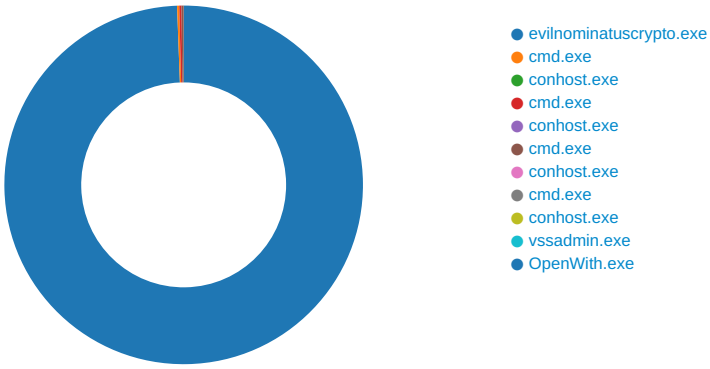
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	1.0.8079.11358
InternalName	EvilNominatusCrypto.exe
FileVersion	1.0.8079.11358
ProductName	TRS
ProductVersion	1.0.8079.11358
FileDescription	TRS
OriginalFilename	EvilNominatusCrypto.exe

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: evilnominatuscrypto.exe PID: **6516**, Parent PID: **5956**

General

Target ID:	1
Start time:	10:01:56
Start date:	15/02/2022
Path:	C:\Users\user\Desktop\evilnominatuscrypto.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\evilnominatuscrypto.exe"
Imagebase:	0x170000
File size:	32768 bytes
MD5 hash:	7CDF50EE4F3D0FEBC70DD36298ED07DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Voidcrypt, Description: Yara detected Voidcrypt Ransomware, Source: 00000001.00000002.880899143.0000000002421000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **6832**, Parent PID: **6516**

General

Target ID:	5
Start time:	10:02:12
Start date:	15/02/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C echo ^[autorun^] >autorun.inf
Imagebase:	0x2a0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2AD194	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	0	12	5b 61 75 74 6f 72 75 6e 5d 20 0d 0a	[autorun]	success or wait	1	2B2837	WriteFile

Analysis Process: conhost.exe PID: **6912**, Parent PID: **6832**

General

Target ID:	6
Start time:	10:02:14
Start date:	15/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **6956**, Parent PID: **6516**

General

Target ID:	7
Start time:	10:02:15
Start date:	15/02/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C echo ^open^=KasperskyScan^.exe >>autorun.inf
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	12	25	6f 70 65 6e 3d 4b 61 73 70 65 72 73 6b 79 53 63 61 6e 2e 65 78 65 20 0d 0a	open=KasperskyScan.exe	success or wait	1	2B2837	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	unknown	1	success or wait	1	2AD2A9	ReadFile

Analysis Process: conhost.exe PID: **6968**, Parent PID: **6956**

General

Target ID:	8
Start time:	10:02:16
Start date:	15/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **7004**, Parent PID: **6516**

General

Target ID:	9
Start time:	10:02:17
Start date:	15/02/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C echo ^execute=^KasperskyScan^.exe >>autorun.inf
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	37	28	65 78 65 63 75 74 65 3d 4b 61 73 70 65 72 73 6b 79 53 63 61 6e 2e 65 78 65 20 0d 0a	execute=KasperskyScan.exe	success or wait	1	2B2837	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\autorun.inf	unknown	1	success or wait	1	2AD2A9	ReadFile

Analysis Process: conhost.exe PID: **7016**, Parent PID: **7004**

General	
Target ID:	10
Start time:	10:02:18
Start date:	15/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **7052**, Parent PID: **6516**

General	
Target ID:	11
Start time:	10:02:19
Start date:	15/02/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet && wmic shadowcopy delete
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7060**, Parent PID: **7052**

General	
Target ID:	12
Start time:	10:02:19
Start date:	15/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vssadmin.exe PID: **7092**, Parent PID: **7052**

General

Target ID:	13
Start time:	10:02:20
Start date:	15/02/2022
Path:	C:\Windows\SysWOW64\vssadmin.exe
Wow64 process (32bit):	true
Commandline:	vssadmin delete shadows /all /quiet
Imagebase:	0xca0000
File size:	110592 bytes
MD5 hash:	7E30B94672107D3381A1D175CF18C147
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: OpenWith.exe PID: **5772**, Parent PID: **792**

General

Target ID:	30
Start time:	10:05:34
Start date:	15/02/2022
Path:	C:\Windows\System32\OpenWith.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OpenWith.exe -Embedding
Imagebase:	0x7ff730d40000
File size:	111120 bytes
MD5 hash:	D179D03728E95E040A889F760C1FC402
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly