ID: 876164
Sample Name: 2UoXCbfNSl.msi
Cookbook: default.jbs
Time: 11:40:14
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

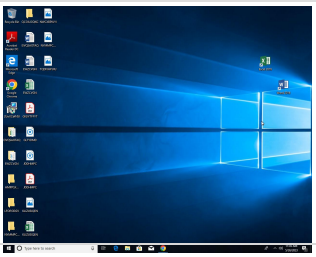
Windows Analysis Report

2UoXCbfNSl.msi

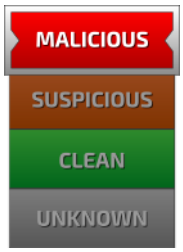
Overview

General Information

Sample Name:	2UoXCbfNSl.msi
Original Sample Name:	cd8393350f7cf…
Analysis ID:	876164
MD5:	82ff84cb9924f0..
SHA1:	df89381239f8a…
SHA256:	cd8393350f7cf…
Tags:	gozi msi
Infos:	



Detection

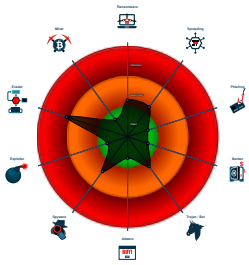


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic
- Drops executables to the windows d…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 5424 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\2UoXCbfNSl.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6800 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6924 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding EA13B634406DD4E4E1EC4CF54DDC47D4 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - MSI2A38.tmp (PID: 2888 cmdline: "C:\Windows\Installer\MSI2A38.tmp" /DontWait C:\Windows\System32\rundll32.exe C:\Users\user\AppData\Roaming\MSTX340\ini.dll,vips MD5: 0007940F5479831428131F029D3BD8F7)
  - MSI2E51.tmp (PID: 5228 cmdline: "C:\Windows\Installer\MSI2E51.tmp" "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" file://C:\Users\user\AppData\Roaming\MSTX340/Information_psw.pdf MD5: 0007940F5479831428131F029D3BD8F7)
- cmd.exe (PID: 6936 cmdline: cmd /c "net group "domain computers" /domain" >> C:\Users\user\AppData\Local\Temp\4505.tmp MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - net.exe (PID: 6948 cmdline: net group "domain computers" /domain MD5: 15534275EDAABC58159DD0F8607A71E5)
    - net1.exe (PID: 6676 cmdline: C:\Windows\system32\net1 group "domain computers" /domain MD5: AF569DE92AB6C1B9C681AF1E799F9983)
- cmd.exe (PID: 2184 cmdline: cmd /c "nltest /dclist:" >> C:\Users\user\AppData\Local\Temp\158A.tmp MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 2820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nltest.exe (PID: 5828 cmdline: nltest /dclist: MD5: 3198EC1CA24B6CB75D597CEE39D71E58)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.865323532023883 05/26/23-11:41:10.481245
SID:	2023883
Source Port:	65323
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.858581532023883 05/26/23-11:43:55.578387
SID:	2023883
Source Port:	58581
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.863446532023883 05/26/23-11:42:04.741109
SID:	2023883
Source Port:	63446
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.860975532023883 05/26/23-11:42:44.239811
SID:	2023883
Source Port:	60975
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.856687532023883 05/26/23-11:44:33.716234
SID:	2023883
Source Port:	56687
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.856682532023883 05/26/23-11:43:20.455009
SID:	2023883
Source Port:	56682
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.861344532023883 05/26/23-11:45:10.193356
SID:	2023883

Source Port:	61344
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

Networking

Snort IDS alert for network traffic

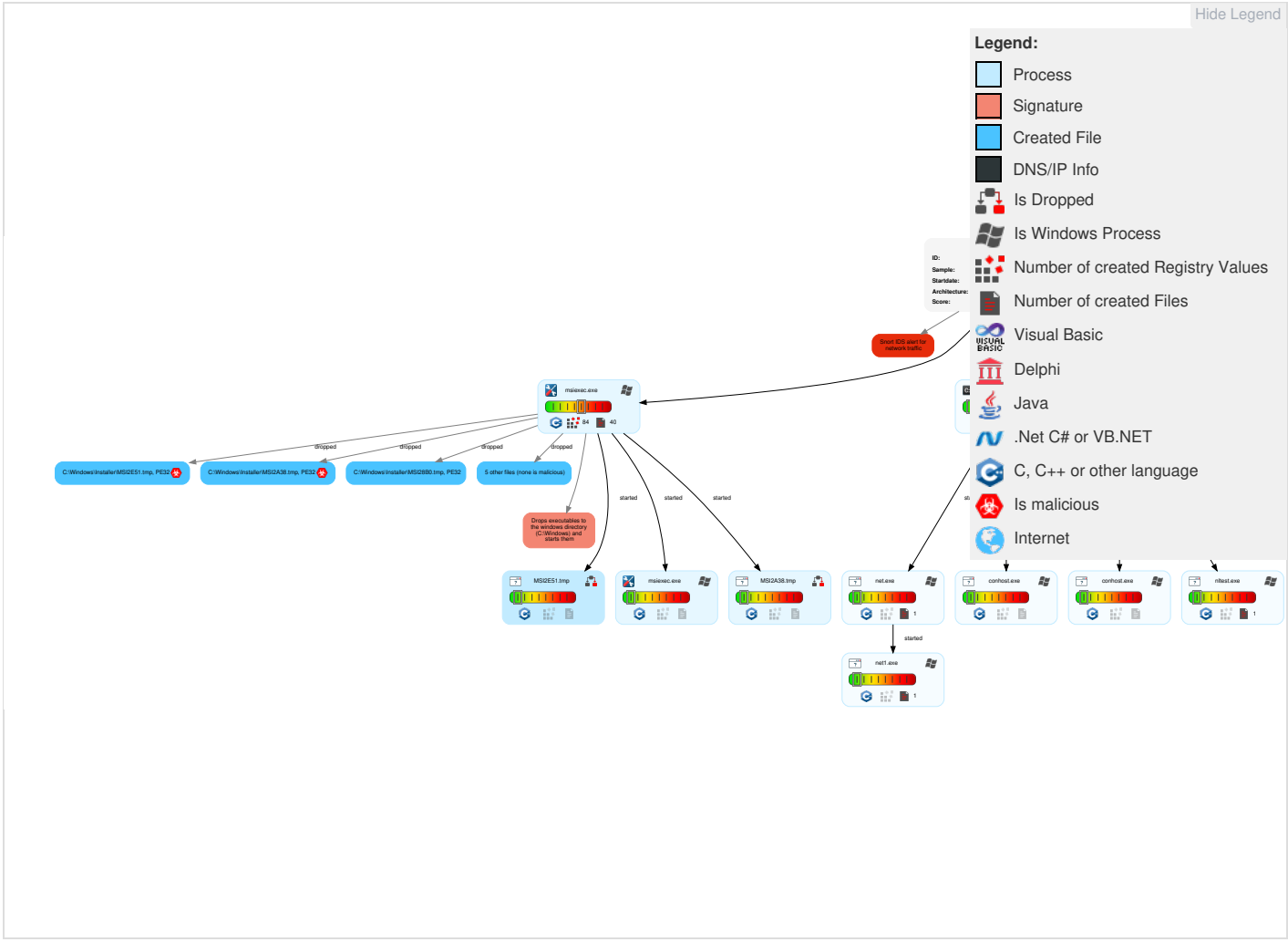
Persistence and Installation Behavior

Drops executables to the windows directory (C:\Windows) and starts them

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
1 Replication Through Removable Media	1 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 2 1 Masquerading	OS Credential Dumping	2 System Time Discovery	1 Replication Through Removable Media	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 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	3 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)	1 DLL Side-Loading	1 1 Process Injection	Security Account Manager	2 Process 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 1 Peripheral Device 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	2 Obfuscated Files or Information	LSA Secrets	1 File and Directory 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 DLL Side-Loading	Cached Domain Credentials	3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

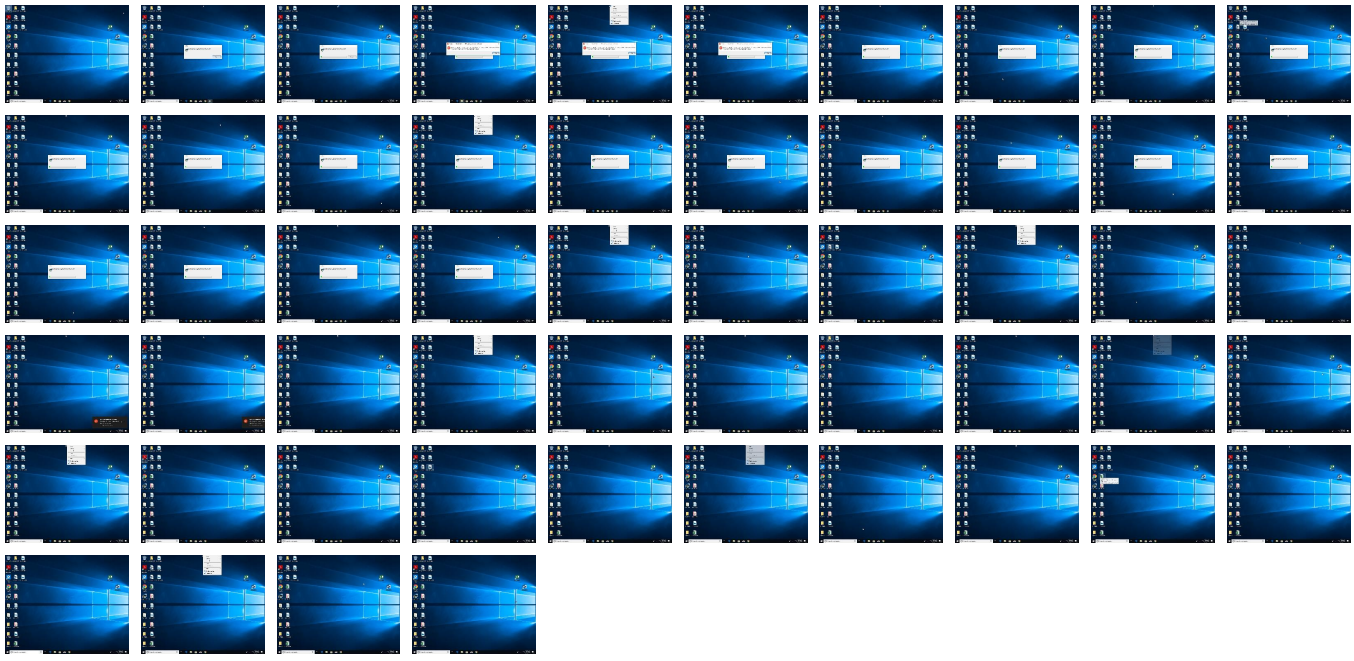
Behavior Graph



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
2UoXCbfNSI.msi	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\MSTX340\ini.dll	0%	ReversingLabs		
C:\Windows\Installer\MSI26B8.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI27A3.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI27E3.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI2841.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI28B0.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI2A38.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI2E51.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.comButtonText_Yes&YesARPCOMMENTSThis	0%	Avira URL Cloud	safe	
http://https://sectigo.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com	51235e.rbs.1.dr, MSI29DA.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.comButtonText_Yes&YesARPCOMMENTSThis	2UoXCbfNSI.msi, 51235f.msi.1.dr, 51235c.msi.1.dr	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876164
Start date and time:	2023-05-26 11:40:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
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
Sample file name:	2UoXCbfNSI.msi
Original Sample Name:	cd8393350f7cfc0762e09ee3b0a98002a1b9abf362caf5f210e717e1d4ebe53a.msi
Detection:	MAL
Classification:	mal52.evad.winMSI@18/31@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 93%) • Quality average: 67.1% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .msi • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, rundll32.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): sumarno.top, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- VT rate limit hit for: 2UoXCbfNSl.msi

Simulations

Behavior and APIs

No simulations

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:\Config.Msi\51235e.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	433224
Entropy (8bit):	6.567843589414793
Encrypted:	false
SSDEEP:	12288:1/ePEitwJH6g7scgFzMzMHf7hM53l6hEFMI:1/EEimJH6g7scSzMQDC51fCI
MD5:	5019AEEF7A712537257F5D833CB69E8E
SHA1:	78E1A5D7A41B0984F9C16F90F887473754ED11F7
SHA-256:	D76A49FAB64EC85290B2524B3C0CFEA2613D80C366C85440B982BF77F08B285E
SHA-512:	E61EE3DA78611724D22617D1A75F9C33B4681B207860A4B0B34737890EBACCFAFD8639F3C14FDF6FF2775C90E40EBC80816CA00464ACCF1A2B3CFE4240CA87 9
Malicious:	false

Preview:	...@IXOS.@.....@%].V.@.....@.....@.....@.....@.....@.....&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}..WinStore..2UoXCbfNSl.msi.@.....@.. ..@.....@.....&.{B4B73A8E-7CF9-43FC-9AD7-95DE9F858356}.....@.....@.....@.....@.....@.....@.....@.....@.....WinStore.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{00A54C1D-61AC-4347-84F4-40773BC436D4}&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}.@.....&.{43A22BE9-40D1-42CF-AB41-12C0C42E4C16}&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}.@.....&.{AB6062B9-9B29-4646-B6E6-7DE312E5AD91}&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}.@.....&.{92907D8E-DBA9-48A2-A3CB-F9F91EE0E4CE}&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}.@.....CreateFolders..Creating folders..Folder: [1]#.4.C:\Users\user\AppData\Roaming\MultiPlast\WinStore\.@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]..(.C:\Users\user\AppData\Roaming\MSTX340\.../.C:\Users\alf

C:\Users\user\AppData\Local\Temp\158A.tmp

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	36
Entropy (8bit):	4.030493056757482
Encrypted:	false
SSDEEP:	3:XT5LzdUA2AGN8y:XtLxUANGN8y
MD5:	C58986635C266E6C06609B908580BEDE
SHA1:	4672DCE03D3DD9560CF74035AFF3D9AEBB7201E4
SHA-256:	A2F1BB2817F976E129974B003E3EC12FB8A644C1952BB667116317FD26416042
SHA-512:	36241E4BDA8AD7E4137624BBFBB999C643D34A2095BA078F9886D92F4726913BDB9DC1E1F44141A6738C1E4D9042B802E49F774C0F1C6901735F4B069834449F
Malicious:	false
Preview:	The command completed successfully..

C:\Users\user\AppData\Local\Temp\4505.tmp

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	78
Entropy (8bit):	4.53413189515719
Encrypted:	false
SSDEEP:	3:GAJzRRljFEOllAEXrkVBiqV9yyn:5zRRl5KAEXoriqX
MD5:	AAEC14B2DE8E2FDAF8427672122AF65C
SHA1:	CA953EFAD669C93AF85B968D747BAA544D4465FB
SHA-256:	14C94C44D0EB89A820D96E1791F4B754C87EE778B5F4478289DF0FB22E1C3DA1
SHA-512:	A5CBAD3DE5070FDCD6AA7F3F5EDA42B69FAEF44A431CF48E20CA1F4F42C648EE80BD5F1D9B981624AE6B39E2435B4278C9FD1E97491E3B244A2BBA7D629021A8
Malicious:	false
Preview:	The request will be processed at a domain controller for domain WORKGROUP.....

C:\Users\user\AppData\Roaming\MSTX340\Information_psw.pdf

Process:	C:\Windows\System32\msiexec.exe
File Type:	PDF document, version 1.5 (zip deflate encoded)
Category:	dropped
Size (bytes):	5025958
Entropy (8bit):	7.900777436536752
Encrypted:	false
SSDEEP:	98304:a4+lkYcmmDre6c12gCZ14CMrCQt+v0UO3KibbbbbbwVukcRVILLleuCQf4RD8:4MmmjBgY10bt+MUOTbbbbbbwZcRVILh9
MD5:	3926092166AE5C4C0366277EF094B9E2
SHA1:	225F6AAD4A6AD7F66B674ED40A0CD67B6FBB6F38
SHA-256:	CD30DA7E64DD8C7FD2F707E54C68BD874AAABC48D2B191C2C7E0AEE9C32888CB
SHA-512:	FB077BDEECC571D631F016DAF7091C2BF440BE5819637825B5D89ED361BF76773F615BD1DEC92BE4207679A83817FC4A1A53ED0AE1A5BB4719B6FD4E842178B
Malicious:	false
Preview:	%PDF-1.5.%.....2444 0 obj.<</Linearized 1/L 5025958/O 2446/E 57616/N 84/T 5024216/H [474 1159]>>.endobj. ..2452 0 obj.<</DecodeParms<</Columns 4/Predictor 12>>/Filter/FlateDecode/ID[<7C60734995C6624C9AEEF51DA7B6A81D><D430149DEEA1D1468BAE56DDABC60FC4>]/Index[2444 17]/Info 2443 0 R/Length 59/Prev 5024217/Root 2445 0 R/Size 2461/Type/XRef/W[1 2 1]>>stream..h.bbd.``b`.....`.....".."...9.A...q...x...0.....endstream.endobj.startxref..0..%%EOF.. ..2460 0 obj.<</C 1427/Filter/FlateDecode/I 1450/Length 1058/O 1411/S 1259>>stream..h..T.O.u..G.\..\[tu.[.*c.."..IL.....`B..P.....V..X....m.(...&.8E.(..=..#Z.....bP...]....{..}.}...w....".4.. ..z.....5.k.`.;....q..A0.9..-;+RR..f.a.....l6s.T..i.UI..>....Z.W..U.ol.>..o.....<.:[.iM.....1sz>S.d.6..8..s.....,.J....\.k..?.....`.r.....v.O~.>x.W.W.M....y.....f.rD.....}.....Z...eM.K.R;.....}..{.?.a.....w...j...+.xuk...|...].u.@kn.[].L....1..1..f..j..a...[.@PL.....1.(G..%BG.tOA..oe..n.&6&

C:\Users\user\AppData\Roaming\MSTX340\ini.dll

Process:	C:\Windows\System32\msiexec.exe

File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	294400
Entropy (8bit):	6.630880578475371
Encrypted:	false
SSDEEP:	6144:YwqnlTIaNrhtD+Cqdoazww2X/4TFEX0Ia:5qln1Y2MTGkl
MD5:	D0584EDCC980EF43E697629ADE83C54B
SHA1:	A68DEEA2D4F40BEF60C7F605BC2AAE9698259E69
SHA-256:	E33A713B96B45E2B2E0DA350C0FDAAF865139607066AADFF3B67B0CED82CA8BC
SHA-512:	917F8206777512BA537C3B67D4E1A31CBF86C690986EF617D5EE34A7818CE09C23067CAAE3D22A9E1FF7DBA0FDF17322F33B579CA0827F19EF0CBABE2F486B5E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X..@X..@X..@Qf.@^..@.v~AZ..@.vzAR..@.v{AP..@.v\|A[..@=xyAY..@=x~A\..@.w~A]..@X.~@...@.w{AW..@.w.AY..@.w.@Y..@.w}AY..@RichX..@.....PE..d....ITb....." ....`.....0O.....[.....#.....P.....p.....text..... ..`.rdata.....@..@.data.....~.....@....pdata...#.....$.....@..@.rsrc.....@..@.reloc.....|.....@..B.....

C:\Windows\Installer\51235c.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {B4B73A8E-7CF9-43FC-9AD7-95DE9F858356}, Number of Words: 10, Subject: WinStore, Author: MultiPlast, Name of Creating Application: WinStore, Template: ;1033, Comments: This installer database contains the logic and data required to install WinStore., Title: Installation Database, Keywords: Installer, MSI, Database, Create Time/Date: Tue Apr 25 16:36:21 2023, Number of Pages: 200
Category:	dropped
Size (bytes):	6096508
Entropy (8bit):	7.8151534308811135
Encrypted:	false
SSDEEP:	98304:ajJzMUpQ/2zKN5DmsQPKEvia5Zld9l4jH43ZnzgB1wLhQNHFRaFUDAQQHk8iQdvk:M5NzKNgsKKE6UZD9l4IZnzgLwLhQNHFd
MD5:	82FF84CB9924F0855A894E75B5D3EDB2
SHA1:	DF89381239F8A8ECECEB697A6A35A573203BAC09
SHA-256:	CD8393350F7CFC0762E09EE3B0A98002A1B9ABF362CAF5F210E717E1D4EBE53A
SHA-512:	416DB643CBFDA60B26BB3EAC8B6A94B148B506BC016D562BC51E085F765400C56412462B42E2E29DCC44FA621349781C1C225081804C528A0A7FD1822663597E
Malicious:	false
Preview:	.....>.....^.....E.....b.....t.....N...O...P...Q...R...S...T...U...V.....<.....!...5..... ...+..."...#...$...%...&...'...(...)...*...2...,...-...../...0...1...6...3...4...=...?...7...8...9...:...;.....,...>.....@...A...B...C...D.....G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\51235f.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {B4B73A8E-7CF9-43FC-9AD7-95DE9F858356}, Number of Words: 10, Subject: WinStore, Author: MultiPlast, Name of Creating Application: WinStore, Template: ;1033, Comments: This installer database contains the logic and data required to install WinStore., Title: Installation Database, Keywords: Installer, MSI, Database, Create Time/Date: Tue Apr 25 16:36:21 2023, Number of Pages: 200
Category:	dropped
Size (bytes):	6096508
Entropy (8bit):	7.8151534308811135
Encrypted:	false
SSDEEP:	98304:ajJzMUpQ/2zKN5DmsQPKEvia5Zld9l4jH43ZnzgB1wLhQNHFRaFUDAQQHk8iQdvk:M5NzKNgsKKE6UZD9l4IZnzgLwLhQNHFd
MD5:	82FF84CB9924F0855A894E75B5D3EDB2
SHA1:	DF89381239F8A8ECECEB697A6A35A573203BAC09
SHA-256:	CD8393350F7CFC0762E09EE3B0A98002A1B9ABF362CAF5F210E717E1D4EBE53A
SHA-512:	416DB643CBFDA60B26BB3EAC8B6A94B148B506BC016D562BC51E085F765400C56412462B42E2E29DCC44FA621349781C1C225081804C528A0A7FD1822663597E
Malicious:	false
Preview:	.....>.....^.....E.....b.....t.....N...O...P...Q...R...S...T...U...V.....<.....!...5..... ...+..."...#...$...%...&...'...(...)...*...2...,...-...../...0...1...6...3...4...=...?...7...8...9...:...;.....,...>.....@...A...B...C...D.....G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\MSI26B8.tmp

Process:	C:\Windows\System32\msiexec.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	598840
Entropy (8bit):	6.4742572330426045
Encrypted:	false
SSDEEP:	12288:JTjOV8EDRaQsUDE2dYu8z5fN8HcsvwaqN:hjOeEMQNLS5W8svwaqN
MD5:	8E565FD81CA10A65CC02E7901A78C95B
SHA1:	1BCA3979C233321AE527D4508CFE9B3BA825DBD3
SHA-256:	7B64112C2C534203BB59CE1A9B7D5390448C045DDA424FB3CFD5878EDB262016
SHA-512:	144BDE89EBA469B32B59F30E7F4D451329C541ED7B556BC60D118C9E2E5CDF148C2275CCA51C4B9355686AEFA16A4B86A26D4C8FE0DD2CF318B97986310959E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..)..)..)..... $.....8.....>....c.....0.....(.....).....A.....(....U.(..). =.(.....(..Rich).....PE..L...W.%d.....!...#.6.....S.....P.....0.....@.....W..(...8`..,.....8=.....g..x...p..... .....@.....P..P.....text....5.....6..... ..`.rdata...+...P...,..:.....@..@.data... %.....f.....@....rsrc.....v.....@..@.reloc...g..... h...~.....@..B..... .....

C:\Windows\Installer\MSI27A3.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	598840
Entropy (8bit):	6.4742572330426045
Encrypted:	false
SSDEEP:	12288:JTjOV8EDRaQsUDE2dYu8z5fN8HcsvwaqN:hjOeEMQNLS5W8svwaqN
MD5:	8E565FD81CA10A65CC02E7901A78C95B
SHA1:	1BCA3979C233321AE527D4508CFE9B3BA825DBD3
SHA-256:	7B64112C2C534203BB59CE1A9B7D5390448C045DDA424FB3CFD5878EDB262016
SHA-512:	144BDE89EBA469B32B59F30E7F4D451329C541ED7B556BC60D118C9E2E5CDF148C2275CCA51C4B9355686AEFA16A4B86A26D4C8FE0DD2CF318B97986310959E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..)..)..)..... $.....8.....>....c.....0.....(.....).....A.....(....U.(..). =.(.....(..Rich).....PE..L...W.%d.....!...#.6.....S.....P.....0.....@.....W..(...8`..,.....8=.....g..x...p..... .....@.....P..P.....text....5.....6..... ..`.rdata...+...P...,..:.....@..@.data... %.....f.....@....rsrc.....v.....@..@.reloc...g..... h...~.....@..B..... .....

C:\Windows\Installer\MSI27E3.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	598840
Entropy (8bit):	6.4742572330426045
Encrypted:	false
SSDEEP:	12288:JTjOV8EDRaQsUDE2dYu8z5fN8HcsvwaqN:hjOeEMQNLS5W8svwaqN
MD5:	8E565FD81CA10A65CC02E7901A78C95B
SHA1:	1BCA3979C233321AE527D4508CFE9B3BA825DBD3
SHA-256:	7B64112C2C534203BB59CE1A9B7D5390448C045DDA424FB3CFD5878EDB262016
SHA-512:	144BDE89EBA469B32B59F30E7F4D451329C541ED7B556BC60D118C9E2E5CDF148C2275CCA51C4B9355686AEFA16A4B86A26D4C8FE0DD2CF318B97986310959E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..)..)..)..... $.....8.....>....c.....0.....(.....).....A.....(....U.(..). =.(.....(..Rich).....PE..L...W.%d.....!...#.6.....S.....P.....0.....@.....W..(...8`..,.....8=.....g..x...p..... .....@.....P..P.....text....5.....6..... ..`.rdata...+...P...,..:.....@..@.data... %.....f.....@....rsrc.....v.....@..@.reloc...g..... h...~.....@..B..... .....

C:\Windows\Installer\MSI2841.tmp

Process:	C:\Windows\System32\msiexec.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	598840
Entropy (8bit):	6.4742572330426045
Encrypted:	false
SSDEEP:	12288:JTjOV8EDRaQsUDE2dYu8z5fN8HcsvwaqN:hjOeEMQNLS5W8svwaqN
MD5:	8E565FD81CA10A65CC02E7901A78C95B
SHA1:	1BCA3979C233321AE527D4508CFE9B3BA825DBD3
SHA-256:	7B64112C2C534203BB59CE1A9B7D5390448C045DDA424FB3CFD5878EDB262016
SHA-512:	144BDE89EBA469B32B59F30E7F4D451329C541ED7B556BC60D118C9E2E5CDF148C2275CCA51C4B9355686AEFA16A4B86A26D4C8FE0DD2CF318B97986310959E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..)..)..)..... $.....8.....>.....c.....0.....(.....).....A.....(....U.(..). =.(.....(..Rich).....PE..L...W.%d......"!...#.6.....S.....P.....0.....@.....W..(...8`..,.....8=.....g..x...p..... .....@.....P..P.....text....5.....6..... ..`.rdata...+...P...,..:.....@..@.data... %.....f.....@....rsrc.....v.....@..@.reloc...g..... h...~.....@..B..... .....

C:\Windows\Installer\MSI28B0.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	598840
Entropy (8bit):	6.4742572330426045
Encrypted:	false
SSDEEP:	12288:JTjOV8EDRaQsUDE2dYu8z5fN8HcsvwaqN:hjOeEMQNLS5W8svwaqN
MD5:	8E565FD81CA10A65CC02E7901A78C95B
SHA1:	1BCA3979C233321AE527D4508CFE9B3BA825DBD3
SHA-256:	7B64112C2C534203BB59CE1A9B7D5390448C045DDA424FB3CFD5878EDB262016
SHA-512:	144BDE89EBA469B32B59F30E7F4D451329C541ED7B556BC60D118C9E2E5CDF148C2275CCA51C4B9355686AEFA16A4B86A26D4C8FE0DD2CF318B97986310959E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m..)..)..)..... $.....8.....>.....c.....0.....(.....).....A.....(....U.(..). =.(.....(..Rich).....PE..L...W.%d......"!...#.6.....S.....P.....0.....@.....W..(...8`..,.....8=.....g..x...p..... .....@.....P..P.....text....5.....6..... ..`.rdata...+...P...,..:.....@..@.data... %.....f.....@....rsrc.....v.....@..@.reloc...g..... h...~.....@..B..... .....

C:\Windows\Installer\MSI29DA.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	426852
Entropy (8bit):	6.559397164118567
Encrypted:	false
SSDEEP:	12288:1/ePEitwJH6g7scgFzMzMHf7hM53l6hEFMF:1/EEimJH6g7scSzMQDC51fCF
MD5:	0CB5A74785F2E7579793EE98BC1F6C73
SHA1:	3A4B62BC783F4078C2ECEC6FBC73544846BFB5C5
SHA-256:	CC788E81F0089BCE361227390954CD673EC2C54D8C645C4904F7F2EC422FA008
SHA-512:	966A73C53D9EE2CB1BD00BC4282BE5021645A80E495F91A8648557431EB4C09A92463FDE08999F9F8628D6688F60F14FFA50DEAEABA528BE917EA214FE349808
Malicious:	false
Preview:	...@IXOS.@.....@%].V.@.....@.....@.....@.....@.....@.....&.{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}..WinStore..2UoXCbfNSI.msi.@.....@.. ..@.....@.....&.{B4B73A8E-7CF9-43FC-9AD7-95DE9F858356}.....@.....@.....@.....@.....@.....@.....@.....@.....WinStore.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration...@.....@.....@.].....&.{00A54C1D-61AC-4347-84F4-40773BC436D4}4.C:\Users\user\AppData\Roaming\MultiPlast\WinStore\.@.....@.....@.....@.....&.{43A22BE9-40D1-42CF-AB41-12C0C42E4C16}(.01:\Software\MultiPlast\WinStore\Version.@.....@.....@.....@.....&.{AB6062B9-9B29-4646-B6E6-7DE312E5AD91}/.C:\Users\user\AppData\Roaming\MSTX340\ini.dll.@.....@.....@.....@.....&.{92907D8E-DBA9-48A2-A3CB-F9F91EE0E4CE};.C:\Users\user\AppData\Roaming\MSTX340\Information_psw.pdf.@.....@.....@.....@.....CreateFolders..Creating folders..Folder: [1]".4.C:\Users\user\AppData\Roaming\M

C:\Windows\Installer\MSI2A38.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	423936
Entropy (8bit):	6.554120162469703
Encrypted:	false
SSDEEP:	12288:A/ePEitwJH6g7scgFzMzMHf7hM53l6hEFM:A/EEimJH6g7scSzMQDC51fC
MD5:	0007940F5479831428131F029D3BD8F7
SHA1:	8DED66ACBD836388C1414512025BD9004C90903B
SHA-256:	340B6EECEB447FB9C8393DDAAA896C9D7013333E2D5587C7A580E56BEB232320
SHA-512:	C4F75C939ACF139F85ABFFC0264DE0279EF35914121E132C0BC22B3EA0080A9573665080F5C8AE5DB3B620341AACC871D094EF52BC7B6963275112572A490BD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.5..g[..g[..g[...X.rg[...^..g[..._.lg[...X.hg[...^./g[..._.hg[...].~g[...Z.fg[..g Z..g[...R.eg[.....~g[..g.~g[...Y.~g[.Rich.g[.....PE..L...q.%d....."....#.....@.....SL....@.....p..8..... ....:..(...p.....h...@.....I.....text..... ..`.rdata...R.....T.....@..@.data....7...0.....@....rsrc...8....p.....0..... ..@..@.reloc...:.....<...<.....@..B..... .....

C:\Windows\Installer\MSI2E51.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	423936
Entropy (8bit):	6.554120162469703
Encrypted:	false
SSDEEP:	12288:A/ePEitwJH6g7scgFzMzMHf7hM53l6hEFM:A/EEimJH6g7scSzMQDC51fC
MD5:	0007940F5479831428131F029D3BD8F7
SHA1:	8DED66ACBD836388C1414512025BD9004C90903B
SHA-256:	340B6EECEB447FB9C8393DDAAA896C9D7013333E2D5587C7A580E56BEB232320
SHA-512:	C4F75C939ACF139F85ABFFC0264DE0279EF35914121E132C0BC22B3EA0080A9573665080F5C8AE5DB3B620341AACC871D094EF52BC7B6963275112572A490BD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.5..g[..g[..g[...X.rg[...^..g[..._.lg[...X.hg[...^./g[..._.hg[...].~g[...Z.fg[..g Z..g[...R.eg[.....~g[..g.~g[...Y.~g[.Rich.g[.....PE..L...q.%d....."....#.....@.....SL....@.....p..8..... ....:..(...p.....h...@.....I.....text..... ..`.rdata...R.....T.....@..@.data....7...0.....@....rsrc...8....p.....0..... ..@..@.reloc...:.....<...<.....@..B..... .....

C:\Windows\Installer\SourceHash{61FBEA40-2644-43BA-811E-2B6E5B7CAA2A}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1643312877601788
Encrypted:	false
SSDEEP:	12:JSbX72Fj6UAGiLIlHVRpZh/77777777777777777777777vDHFXEcNuit/l0i5:J7QI5tx3iF
MD5:	EFB3328B4DE134D0E78A76334A84596D
SHA1:	7995922AEB32005BEB2E17E21E85A654A19B8593
SHA-256:	D1E96F12D9544F06CBCE473F6F1F90A484B1BD59BA5DC50E05133B93B04920CA
SHA-512:	74FACAA1185467BC7516B2969D39062AB7CA1BC3F7AF0E356588B778D8E58F4E96A223C47FBAC7B9303D65BAE7EB0A1A53F798170CC4A227E91B4F01879B813 9
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5303886579335395

Encrypted:	false
SSDEEP:	48:k8PhquRc06WXJWFT5JBFrSZFAErCykxrSZZThIH:7hq1tFT3BFr4OwCdr4E
MD5:	5A26ADF205D266FD71C7F863D5E2938D
SHA1:	434D819B840D50770E6E85EEE5AC251D12F5439D
SHA-256:	4CAC64CE59CBD07DA3FB8E10E533EF264A2E231B05EDB2089793D9C88F976286
SHA-512:	FFA27B08779C87E6D54FF98D6805EE10E7EAEFAB04E0C86FBCEEB7A64F8254CF436851250B288B82B2F4FDBA8F63BD9D9B4A595ADFA0B6AABD38AB2C70A3CC88
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	81287
Entropy (8bit):	5.298770088687002
Encrypted:	false
SSDEEP:	192:XL/vcrZZDZo/ZrXczaIcO/gcMH5elWSLK:XDvsDZGrkaIcO/Y5XuK
MD5:	E84CEBF763C0BF4948BC6B99286B5479
SHA1:	EFB268A1C5DC2CAA1F2EB69747025E50F46765CA
SHA-256:	53EE78262CD145E9EEAFCBE8DA3DB5DAE242A6DF75832F431DE2D5AB538D5489
SHA-512:	26B52EE7A321FA084B239E0B1FB81BB9B163C4EF0ADC11C60D33D33663F661D85C73987AF4AB6BE0D25A9360527DD845C76CCFFAE3D305A03C368F643CDE5176
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:38:04.497 [4552]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.513 [4552]: ngen returning 0x00000000..07/23/2020 10:38:04.559 [4480]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.559 [4480]: ngen returning 0x00000000..07/23/2020 10:38:04.622 [4256]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.622 [

C:\Windows\Temp\~DF10D2DAB67DA41C8A.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2299014095130887
Encrypted:	false
SSDEEP:	48:73iuPO+CFXJXT5xBFrSZFAErCykxrSZZThIH:jif/TPBFr4OwCdr4E
MD5:	A7BC4B3A3E89C185686F43FA605B9B8D
SHA1:	6BC073D16D83BF863862C3B86F052AC5929F0AB3
SHA-256:	B3D5B044FD2DD2F081E8E52EAB1FA572EC181A1D0DA30622449289F5C1307DE7
SHA-512:	AB9C4C66EF8128B642E86B4C98A1897804D8B2992DB389E22A7A56BBF73A8FA4DBA8724E422C8EFE06DBC04D573C80FA6889F60BA672CA335D8D43238A62BD25
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF1227C6BDFAEB717C.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5303886579335395
Encrypted:	false
SSDEEP:	48:k8PhquRc06WXJWFT5JBFrSZFAErCykxrSZZThIH:7hq1tFT3BFr4OwCdr4E
MD5:	5A26ADF205D266FD71C7F863D5E2938D

SHA1:	434D819B840D50770E6E85EEE5AC251D12F5439D
SHA-256:	4CAC64CE59CBD07DA3FB8E10E533EF264A2E231B05EDB2089793D9C88F976286
SHA-512:	FFA27B08779C87E6D54FF98D6805EE10E7EAEFAB04E0C86FBCEEB7A64F8254CF436851250B288B82B2F4FDBA8F63BD9D9B4A595ADFA0B6AABD38AB2C70A3CC88
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF68D74EC899244EDA.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DF7FE13E1A7726FEE7.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2299014095130887
Encrypted:	false
SSDEEP:	48:73iuPO+CFXJXT5xBFrSZFAErCykxrSZZThIH:jif/TPBFr4OwCdr4E
MD5:	A7BC4B3A3E89C185686F43FA605B9B8D
SHA1:	6BC073D16D83BF863862C3B86F052AC5929F0AB3
SHA-256:	B3D5B044FD2DD2F081E8E52EAB1FA572EC181A1D0DA30622449289F5C1307DE7
SHA-512:	AB9C4C66EF8128B642E86B4C98A1897804D8B2992DB389E22A7A56BBF73A8FA4DBA8724E422C8EFE06DBC04D573C80FA6889F60BA672CA335D8D43238A62BD25
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Temp\~DF8512FFC219F00200.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07172138949471873
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOXEcNVfgVky6lit/:2F0i8n0itFzDHFXEcNBit/
MD5:	2A4834F747E9222F78EE8405FD0997E1
SHA1:	4BF2D081A93F6B6B3613D7A51CD425ACB4984DB9
SHA-256:	FA9E61F246D4781A93A9F597C06F7F8DE30E7E6990984A852A5C5BD2DC7B5E4A
SHA-512:	7C98D68920BB69CF3B0BEB63380C84F331B93158AE723B5DA05175CB5F23FD90357FC33B13FEC95F4B51B057BE3685492F21CB77F494597DD1CBBD8AFF6528CE
Malicious:	false

Preview:	.....

C:\Windows\Temp\~DF95C513D54DE54DBD.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DF96E1B63E07A25412.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	0.12531497003687206
Encrypted:	false
SSDEEP:	24:wAYnXLAMTx0EDripV0EDF0EDripV0EDFAEV0yjCykVQwGBVyR+suC:wHkMTNrSZprSZFAErCyk1I
MD5:	203268CF52A6C032ED29188A6BA2F596
SHA1:	41027384693A91DB4DB44A9FEE45B06042C58E78
SHA-256:	1E6F61F2E3C54149C55EF47F1C9464A0B1FD7AE7AE5655E063F6389652AF29BE
SHA-512:	D868CD9BADE8C235320CA52ACA0B874BD565EAE2A89E83822EAB8A8A4FBB0F5C5D86C211A36F6472CCA1B0BE8AD212D7726F1D65FB0707FDA96B13EB2A31EF5D
Malicious:	false
Preview:	.....

C:\Windows\Temp\~DFB2AA96E7FD83FBD9.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5303886579335395
Encrypted:	false
SSDEEP:	48:k8PhquRc06WXJWFT5JBFrSZFAErCykxrSZZThIH:7hq1tFT3BFr4OwCdr4E
MD5:	5A26ADF205D266FD71C7F863D5E2938D
SHA1:	434D819B840D50770E6E85EEE5AC251D12F5439D
SHA-256:	4CAC64CE59CBD07DA3FB8E10E533EF264A2E231B05EDB2089793D9C88F976286
SHA-512:	FFA27B08779C87E6D54FF98D6805EE10E7EAEFAB04E0C86FBCEEB7A64F8254CF436851250B288B82B2F4FDBA8F63BD9D9B4A595ADFA0B6AABD38AB2C70A3CC88
Malicious:	false
Preview:	.....>.....

C:\Windows\Temp\~DFB34D19DFF552AF61.TMP

Process:	C:\Windows\System32\msiexec.exe

File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFBED5ECD771A438C3.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFDDFB5948BDA3D3DB.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Windows\Temp\~DFE5C2C184C7DA67D2.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.2299014095130887
Encrypted:	false
SSDEEP:	48:73iuPO+CFXJXT5xBFrSZFAErCykxrSZZThlH:jif/TPBFr4OwCdr4E
MD5:	A7BC4B3A3E89C185686F43FA605B9B8D
SHA1:	6BC073D16D83BF863862C3B86F052AC5929F0AB3
SHA-256:	B3D5B044FD2DD2F081E8E52EAB1FA572EC181A1D0DA30622449289F5C1307DE7

SHA-512:	AB9C4C66EF8128B642E86B4C98A1897804D8B2992DB389E22A7A56BBF73A8FA4DBA8724E422C8EFE06DBC04D573C80FA6889F60BA672CA335D8D43238A62BD25
Malicious:	false
Preview:	.....>..... ....

\Device\ConDrv

Process:	C:\Windows\System32\nltest.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.8791536144029335
Encrypted:	false
SSDEEP:	3:YaHNFdAmER2fQsKKrqyav:YQNs92Sfv
MD5:	45B19A8643D9F754F189A9B397DF3722
SHA1:	4A9C4C1A875E5C98353DA157493ED0B4C0A653B5
SHA-256:	BEA3B5810B84EE81FB257645355539BC9BEFA02E457EC4E359BEC21C2BEEB042
SHA-512:	A676AD5D35BE590BC52613499CE6E00452D64C2681E3C23A831BD886350C8EF54BE74FE78A7C6C7ED4984EFFC92F8F7E86B1FD564759156D5A7B288A5754BF38
Malicious:	false
Preview:	Cannot find DC to get DC list from.Status = 1355 0x54b ERROR_NO_SUCH_DOMAIN..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {B4B73A8E-7CF9-43FC-9AD7-95DE9F858356}, Number of Words: 10, Subject: WinStore, Author: MultiPlast, Name of Creating Application: WinStore, Template: ;1033, Comments: This installer database contains the logic and data required to install WinStore., Title: Installation Database, Keywords: Installer, MSI, Database, Create Time/Date: Tue Apr 25 16:36:21 2023, Number of Pages: 200
Entropy (8bit):	7.8151534308811135
TrID:	• Microsoft Windows Installer (77509/1) 52.18% • Windows SDK Setup Transform Script (63028/2) 42.43% • Generic OLE2 / Multistream Compound File (8008/1) 5.39%
File name:	2UoXCbfNSl.msi
File size:	6096508
MD5:	82ff84cb9924f0855a894e75b5d3edb2
SHA1:	df89381239f8a8ececeb697a6a35a573203bac09
SHA256:	cd8393350f7cfc0762e09ee3b0a98002a1b9abf362caf5f210e717e1d4ebe53a
SHA512:	416db643cbfda60b26bb3eac8b6a94b148b506bc016d562bc51e085f765400c56412462b42e2e29dcc44fa621349781c1c225081804c528a0a7fd1822663597b
SSDEEP:	98304:ajJzMUpQ/2zKN5DmsQPKEvia5Zld9l4jH43ZnzgB1wLhQNHFRaFUDAQQHk8iQdvk:M5NzKNgsKKE6UZD9l4IZnzgLwLhQNHFd
TLSH:	36561222B2C3C532C55D0277E968FE5E0539BE73473101E777E9396E99B48C1A27AB02
File Content Preview:	.....>.....^.....E.....b.....t.....N...O...P...Q...R...S...T...U...V..... ..

File Icon

Icon Hash:	2d2e3797b32b2b99

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:41:12.081121922 CEST	53	65323	8.8.8.8	192.168.2.5
May 26, 2023 11:42:19.971673965 CEST	53	56751	8.8.8.8	192.168.2.5

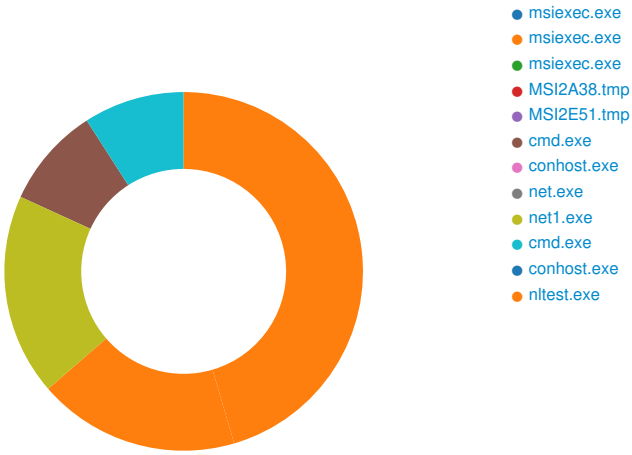
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:42:20.961313963 CEST	53	56751	8.8.8.8	192.168.2.5
May 26, 2023 11:42:45.269511938 CEST	53	60975	8.8.8.8	192.168.2.5
May 26, 2023 11:43:10.349685907 CEST	53	55068	8.8.8.8	192.168.2.5
May 26, 2023 11:43:11.648736954 CEST	53	55068	8.8.8.8	192.168.2.5
May 26, 2023 11:43:21.521276951 CEST	53	56682	8.8.8.8	192.168.2.5
May 26, 2023 11:43:23.114259005 CEST	53	56682	8.8.8.8	192.168.2.5
May 26, 2023 11:43:32.659657955 CEST	53	58532	8.8.8.8	192.168.2.5
May 26, 2023 11:43:56.697468042 CEST	53	58581	8.8.8.8	192.168.2.5
May 26, 2023 11:43:57.602169991 CEST	53	58581	8.8.8.8	192.168.2.5
May 26, 2023 11:44:34.737889051 CEST	53	56687	8.8.8.8	192.168.2.5
May 26, 2023 11:44:46.149173021 CEST	53	64419	8.8.8.8	192.168.2.5
May 26, 2023 11:45:11.309842110 CEST	53	61344	8.8.8.8	192.168.2.5

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 11:41:12.081121922 CEST	8.8.8.8	192.168.2.5	0x2b56	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:42:19.971673965 CEST	8.8.8.8	192.168.2.5	0x698c	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:42:20.961313963 CEST	8.8.8.8	192.168.2.5	0x698c	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:42:45.269511938 CEST	8.8.8.8	192.168.2.5	0xb958	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:10.349685907 CEST	8.8.8.8	192.168.2.5	0x66ae	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:11.648736954 CEST	8.8.8.8	192.168.2.5	0x66ae	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:21.521276951 CEST	8.8.8.8	192.168.2.5	0xe540	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:23.114259005 CEST	8.8.8.8	192.168.2.5	0xe540	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:32.659657955 CEST	8.8.8.8	192.168.2.5	0x8abb	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:56.697468042 CEST	8.8.8.8	192.168.2.5	0xd13c	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:43:57.602169991 CEST	8.8.8.8	192.168.2.5	0xd13c	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:44:34.737889051 CEST	8.8.8.8	192.168.2.5	0x769	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:44:46.149173021 CEST	8.8.8.8	192.168.2.5	0x54ff	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false
May 26, 2023 11:45:11.309842110 CEST	8.8.8.8	192.168.2.5	0xab75	Server failure (2)	sumarno.top	none	none	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: 5424, Parent PID: 3324

General

Target ID:	0
Start time:	11:41:06
Start date:	26/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\2UoXCbfNSI.msi"
Imagebase:	0x7ff79d900000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6800, Parent PID: 564

General

Target ID:	1
Start time:	11:41:06
Start date:	26/05/2023
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff79d900000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
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 Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	81193	94	30 35 2f 32 36 2f 32 30 32 33 20 31 31 3a 34 31 3a 30 37 2e 39 30 32 20 5b 36 38 30 30 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	05/26/2023 11:41:07.902 [6800]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFA04DEBEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFA04DEBBC6	ReadFile

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

Analysis Process: msiexec.exe PID: **6924**, Parent PID: **6800**

General

Target ID:	2
Start time:	11:41:08
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding EA13B634406DD4E4E1EC4CF54DDC47D4
Imagebase:	0x11f0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSI2A38.tmp PID: **2888**, Parent PID: **6800**

General

Target ID:	3
Start time:	11:41:09
Start date:	26/05/2023
Path:	C:\Windows\Installer\MSI2A38.tmp
Wow64 process (32bit):	true

Commandline:	"C:\Windows\Installer\MSI2A38.tmp" /DontWait C:\Windows\System32\rundll32.exe C:\Users\user\AppData\Roaming\MSTX340\ini.dll,vips
Imagebase:	0x1320000
File size:	423936 bytes
MD5 hash:	0007940F5479831428131F029D3BD8F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MSI2E51.tmp PID: 5228, Parent PID: 6800

General

Target ID:	5
Start time:	11:41:10
Start date:	26/05/2023
Path:	C:\Windows\Installer\MSI2E51.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Installer\MSI2E51.tmp" "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" file://C:\Users\user\AppData\Roaming\MSTX340/Information_psw.pdf
Imagebase:	0x1180000
File size:	423936 bytes
MD5 hash:	0007940F5479831428131F029D3BD8F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6936, Parent PID: 5260

General

Target ID:	8
Start time:	11:41:55
Start date:	26/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c "net group "domain computers" /domain" >> C:\Users\user\AppData\Local\Temp\4505.tmp
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
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\AppData\Local\Temp\4505.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF62773C614	CreateFileW

Analysis Process: conhost.exe PID: **7020**, Parent PID: **6936**

General	
Target ID:	9
Start time:	11:41:55
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: net.exe PID: **6948**, Parent PID: **6936**

General	
Target ID:	10
Start time:	11:41:55
Start date:	26/05/2023
Path:	C:\Windows\System32\net.exe
Wow64 process (32bit):	false
Commandline:	net group "domain computers" /domain
Imagebase:	0x7ff737ac0000
File size:	56832 bytes
MD5 hash:	15534275EDAABC58159DD0F8607A71E5
Has elevated privileges:	false
Has administrator privileges:	false
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: net1.exe PID: **6676**, Parent PID: **6948**

General	
Target ID:	11
Start time:	11:41:55
Start date:	26/05/2023
Path:	C:\Windows\System32\net1.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\net1 group "domain computers" /domain
Imagebase:	0x7ff734b00000
File size:	175104 bytes

MD5 hash:	AF569DE92AB6C1B9C681AF1E799F9983
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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\AppData\Local\Temp\4505.tmp	0	76	54 68 65 20 72 65 71 75 65 73 74 20 77 69 6c 6c 20 62 65 20 70 72 6f 63 65 73 73 65 64 20 61 74 20 61 20 64 6f 6d 61 69 6e 20 63 6f 6e 74 72 6f 6c 6c 65 72 20 66 6f 72 20 64 6f 6d 61 69 6e 20 57 4f 52 4b 47 52 4f 55 50 2e 0d 0a	The request will be processed at a domain controller for domain WORKGROUP.	success or wait	1	7FF734B1C73A	WriteFile
C:\Users\user\AppData\Local\Temp\4505.tmp	76	2	0d 0a		success or wait	1	7FF734B1C73A	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2184**, Parent PID: **5260**

General

Target ID:	12
Start time:	11:42:09
Start date:	26/05/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c "nltest /dclist:" >> C:\Users\user\AppData\Local\Temp\158A.tmp
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\158A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF62773C614	CreateFileW

Analysis Process: conhost.exe PID: **2820**, Parent PID: **2184**

General

Target ID:	13
Start time:	11:42:09
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: nltest.exe PID: **5828**, Parent PID: **2184**

General

Target ID:	14
Start time:	11:42:09
Start date:	26/05/2023
Path:	C:\Windows\System32\nltest.exe
Wow64 process (32bit):	false
Commandline:	nltest /dclist:
Imagebase:	0x7ff6e1400000
File size:	514048 bytes
MD5 hash:	3198EC1CA24B6CB75D597CEE39D71E58
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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
\Device\ConDrv	35	35	53 74 61 74 75 73 20 3d 20 31 33 35 35 20 30 78 35 34 62 20 45 52 52 4f 52 5f 4e 4f 5f 53 55 43 48 5f 44	Status = 1355 0x54b ERROR_NO_SUCH_D	success or wait	1	7FF6E1408253	WriteFile
\Device\ConDrv	54	19	20 45 52 52 4f 52 5f 4e 4f 5f 53 55 43 48 5f 44 4f 4d 41	ERROR_NO_SUCH_DOMA	success or wait	1	7FF6E1408253	WriteFile
\Device\ConDrv	75	21	0d 0a		success or wait	1	7FF6E1408253	WriteFile
\Device\ConDrv	77	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF6E1408253	WriteFile
C:\Users\user\AppData\Local\Temp\158A.tmp	0	36	54 68 65 20 63 6f 6d 6d 61 6e 64 20 63 6f 6d 70 6c 65 74 65 64 20 73 75 63 63 65 73 73 66 75 6c 6c 79 0d 0a	The command completed successfully	success or wait	1	7FF6E1408253	WriteFile

Disassembly

No disassembly