



ID: 595302
Sample Name: IMqJSR2NIi
Cookbook: default.jbs
Time: 15:39:43
Date: 23/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report IMqJSR2NIi 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
System Summary 5
Joe Sandbox Signatures 5
AV Detection 5
E-Banking Fraud 5
HIPS / PFW / Operating System Protection Evasion 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
World Map of Contacted IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 12
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe 12
C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll 12
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll 12
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe 13
C:\Users\user\AppData\Local\OiZS\SLC.dll 13
C:\Users\user\AppData\Local\OiZS\msinfo32.exe 13
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe 14
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll 14
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll 14
C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe 15
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll 15
C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe 15
C:\Users\user\AppData\Local\Zc3\NETPLWIZ.dll 16
C:\Users\user\AppData\Local\Zc3\Netplwiz.exe 16
C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe 16
C:\Users\user\AppData\Local\f3fc\appwiz.cpl 17
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL 17
C:\Users\user\AppData\Local\jOnYG\mfpmp.exe 18
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll 18
C:\Users\user\AppData\Local\p9w993CR\msra.exe 18
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a 19
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Data Directories 21
Sections 21
Resources 24
Imports 24

Exports 24
Version Infos 24
Possible Origin 24
Network Behavior 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: loaddll64.exePID: 6600, Parent PID: 3104 25
General 25
File Activities 26
Analysis Process: cmd.exePID: 6608, Parent PID: 6600 26
General 26
File Activities 26
Analysis Process: rundll32.exePID: 6616, Parent PID: 6600 26
General 26
File Activities 26
File Read 26
Analysis Process: rundll32.exePID: 6628, Parent PID: 6608 27
General 27
File Activities 27
File Read 27
Analysis Process: explorer.exePID: 3616, Parent PID: 6616 27
General 27
File Activities 27
File Created 27
File Deleted 29
File Written 30
File Read 40
Registry Activities 41
Key Created 41
Key Value Created 42
Analysis Process: rundll32.exePID: 6768, Parent PID: 6600 42
General 42
File Activities 43
File Read 43
Analysis Process: rundll32.exePID: 6932, Parent PID: 6600 43
General 43
File Activities 43
File Read 43
Analysis Process: msra.exePID: 6316, Parent PID: 3616 43
General 43
Analysis Process: msra.exePID: 5220, Parent PID: 3616 43
General 43
File Activities 44
File Read 44
Analysis Process: mfpmp.exePID: 6676, Parent PID: 3616 44
General 44
Analysis Process: mfpmp.exePID: 6904, Parent PID: 3616 44
General 44
File Activities 44
File Read 44
Analysis Process: Netplwiz.exePID: 7052, Parent PID: 3616 45
General 45
Analysis Process: Netplwiz.exePID: 7060, Parent PID: 3616 45
General 45
File Activities 45
File Read 45
Analysis Process: RecoveryDrive.exePID: 5576, Parent PID: 3616 45
General 45
Analysis Process: RecoveryDrive.exePID: 5760, Parent PID: 3616 46
General 46
File Activities 46
File Read 46
Analysis Process: OptionalFeatures.exePID: 3800, Parent PID: 3616 46
General 46
Analysis Process: OptionalFeatures.exePID: 6096, Parent PID: 3616 46
General 46
Analysis Process: Netplwiz.exePID: 60, Parent PID: 3616 47
General 47
Analysis Process: Netplwiz.exePID: 3948, Parent PID: 3616 47
General 47
Analysis Process: MusNotificationUx.exePID: 2108, Parent PID: 3616 47
General 47
Analysis Process: MusNotificationUx.exePID: 3600, Parent PID: 3616 47
General 48
Analysis Process: wscript.exePID: 4220, Parent PID: 3616 48
General 48
Analysis Process: wscript.exePID: 6152, Parent PID: 3616 48
General 48
Analysis Process: DevicePairingWizard.exePID: 4956, Parent PID: 3616 48
General 48
Disassembly 49

Copyright Joe Security LLC 2022

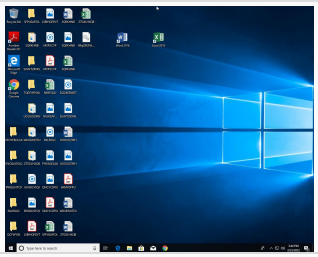
Windows Analysis Report

IMqJSR2NIi

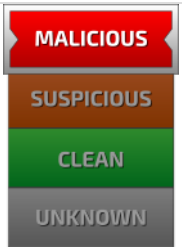
Overview

General Information

Sample Name:	IMqJSR2NIi (renamed file extension from none to dll)
Analysis ID:	595302
MD5:	26c6fe63e7b7dd..
SHA1:	8787e8c20838ee..
SHA256:	9303d54f40b9c7..
Tags:	Dridex exe
Infos:	



Detection



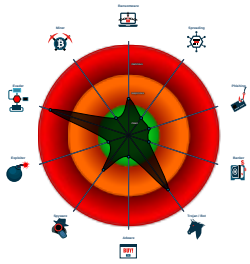
Dridex

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

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Queues an APC in another process …
- Sigma detected: Suspicious Call by…
- Machine Learning detection for drop…
- Contains functionality to prevent loc…
- Uses Atom Bombing / ProGate to in…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6600 cmdline: loaddll64.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6608 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6628 cmdline: rundll32.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6616 cmdline: rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingFormatString MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msra.exe (PID: 6316 cmdline: C:\Windows\system32\msra.exe MD5: 3240CC226FB8AC41A0431A8F3B9DD770)
      - msra.exe (PID: 5220 cmdline: C:\Users\user\AppData\Local\p9w993CR\msra.exe MD5: 3240CC226FB8AC41A0431A8F3B9DD770)
      - mfpmp.exe (PID: 6676 cmdline: C:\Windows\system32\mfpmp.exe MD5: 7C3D09D6DB5DB4A272FCF4C1BB3986BD)
      - mfpmp.exe (PID: 6904 cmdline: C:\Users\user\AppData\Local\jOnYG\mfpmp.exe MD5: 7C3D09D6DB5DB4A272FCF4C1BB3986BD)
      - Netplwiz.exe (PID: 7052 cmdline: C:\Windows\system32\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
      - Netplwiz.exe (PID: 7060 cmdline: C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
      - RecoveryDrive.exe (PID: 5576 cmdline: C:\Windows\system32\RecoveryDrive.exe MD5: 2228E677678848E2FC693199947715E7)
      - RecoveryDrive.exe (PID: 5760 cmdline: C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe MD5: 2228E677678848E2FC693199947715E7)
      - OptionalFeatures.exe (PID: 3800 cmdline: C:\Windows\system32\OptionalFeatures.exe MD5: 25FA10F83BEDEF170C9BB47EE7E3CA91)
      - OptionalFeatures.exe (PID: 6096 cmdline: C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe MD5: 25FA10F83BEDEF170C9BB47EE7E3CA91)
      - Netplwiz.exe (PID: 60 cmdline: C:\Windows\system32\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
      - Netplwiz.exe (PID: 3948 cmdline: C:\Users\user\AppData\Local\Zc3\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
      - MusNotificationUx.exe (PID: 2108 cmdline: C:\Windows\system32\MusNotificationUx.exe MD5: 114A55D75AC7447F012B6D8EC8B1F7FC)
      - MusNotificationUx.exe (PID: 3600 cmdline: C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe MD5: 114A55D75AC7447F012B6D8EC8B1F7FC)
      - wscript.exe (PID: 4220 cmdline: C:\Windows\system32\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 6152 cmdline: C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - DevicePairingWizard.exe (PID: 4956 cmdline: C:\Windows\system32\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
  - rundll32.exe (PID: 6768 cmdline: rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingFormatStringForEdition MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6932 cmdline: rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingLoadBitmap MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.426087810.00007FFFF6CD1000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000028.00000002.611239452.00007FFFE3391000.00000020.00000001.01000000.0000001B.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.269553653.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001D.00000002.483809310.00007FFFF0DC1000.00000020.00000001.01000000.00000012.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.254908404.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
26.2.Netplwiz.exe.7ffff6cd0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
29.2.RecoveryDrive.exe.7ffff0dc0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
37.2.MusNotificationUx.exe.7fffe3390000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
33.2.Netplwiz.exe.7ffff6cd0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
19.2.msra.exe.7fffef950000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 8 entries				

Sigma Signatures

System Summary



Sigma detected: Suspicious Call by Ordinal

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud



Yara detected Dridex unpacked file

HIPS / PFW / Operating System Protection Evasion



Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

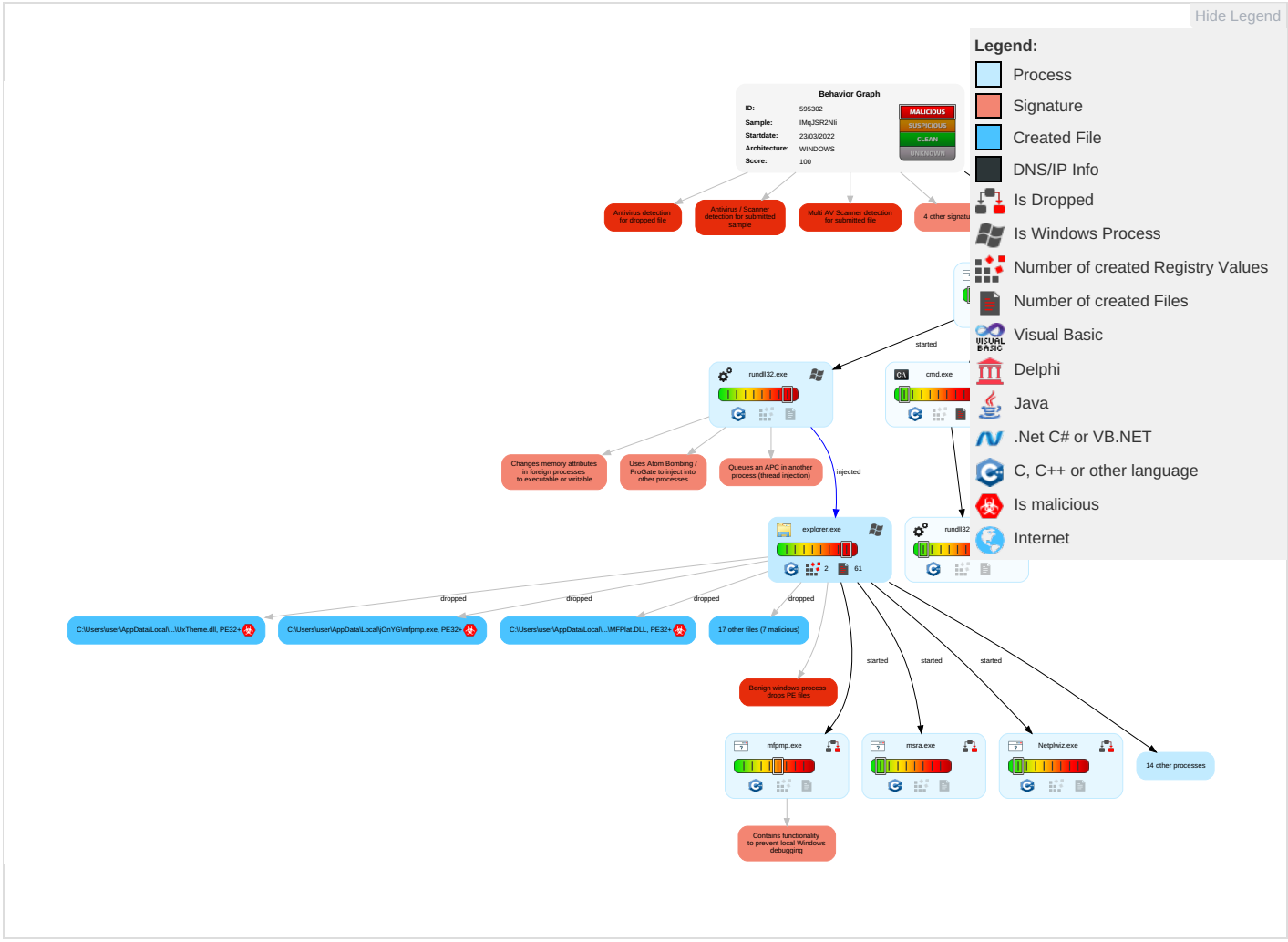
Contains functionality to prevent local Windows debugging

Uses Atom Bombing / ProGate to inject into other processes

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
Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	OS Credential Dumping	1 2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	1 Exploitation for Client Execution	1 Windows Service	1 Access Token Manipulation	3 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	1 System Shutdown/ Reboot
Domain Accounts	2 Service Execution	Logon Script (Windows)	1 Windows Service	2 Software Packing	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)	4 1 2 Process Injection	1 Timestomp	NTDS	3 5 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 DLL Side-Loading	LSA Secrets	1 Query Registry	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 Masquerading	Cached Domain Credentials	3 1 Security Software 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 Virtualization/Sandbox Evasion	DCSync	1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	3 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	4 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			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
IMqJSR2NIi.dll	68%	Virustotal		Browse
IMqJSR2NIi.dll	63%	Metadefender		Browse
IMqJSR2NIi.dll	86%	ReversingLabs	Win64.Trojan.Occamy	
IMqJSR2NIi.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
IMqJSR2NIi.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\f3fc\appwiz.cpl	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	100%	Avira	TR/Crypt.XPACK.Gen7	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\OiZS\SLC.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\f3fc\appwiz.cpl	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\OiZS\SLC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\OiZS\msinfo32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\OiZS\msinfo32.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.2.Netplwiz.exe.21828b10000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
29.2.RecoveryDrive.exe.7ffff0dc0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.Netplwiz.exe.7ffff6cd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.MusNotificationUx.exe.7fffe3390000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.msra.exe.7fffef950000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.Netplwiz.exe.7ffff6cd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.1ec47d00000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
22.2.mfpmp.exe.1f89f070000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
40.2.wscript.exe.7fffe3390000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.7fffe24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.7fffe24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.7fffe24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.RecoveryDrive.exe.1db7dca0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
40.2.wscript.exe.228669c0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
37.2.MusNotificationUx.exe.2785c0e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
33.2.Netplwiz.exe.1c2b90e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
7.2.rundll32.exe.7fffe24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.1f703fe0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
31.2.OptionalFeatures.exe.7ffff6cd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.7fffe24a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.1b90ef60000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
9.2.rundll32.exe.20fef320000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
31.2.OptionalFeatures.exe.1f3e6e00000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
19.2.msra.exe.1bcecc70000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.rundll32.exe.249dba40000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
22.2.mfpmp.exe.7ffff6cd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	595302
Start date and time:	2022-03-23 14:39:43 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IMqJSR2NIi (renamed file extension from none to dll)
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:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@49/21@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 7.5% (good quality ratio 6.3%) • Quality average: 59% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.

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:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	5.664138088677901
Encrypted:	false
SSDEEP:	1536:D/BmrFjio5/vzDSPwiEKi3xGyibqZ3qOT3:9mp5SwiEKWZiTo3
MD5:	E23643C785D498FF73B5C9D7EA173C3D
SHA1:	56296F1D29FC2DCBFAA1D991C87B10968C6D3882
SHA-256:	40F423488FC0C13DED29109F8CC1C0D2CCE52ECB1BD01939EF774FE31014E0F4
SHA-512:	22E29A06F19E2DA941A707B8DA7115E0F5962617295CC36395A8E9B2A98F0239B6519B4BF4AB1DC671DEF8CD558E8F59F4E50C63130D392D1E085BBF6B71091
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a...a...a...h...o.....b.....r.....i.....j...a.....c.....j.`.....`...Richa..... .....PE..d...x.1".....".....\.....b.....@.....H...`..... .....|..T.....`r.....`s..8 .....text....[.....\..... ..`.rdata...-...p.....`.....@..@.data... .....@....pdata.....@..@.rsrc.....@..@.re loc.....f.....@..B..... .....

C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1380352
Entropy (8bit):	5.145457121106975
Encrypted:	false
SSDEEP:	12288:ZZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwB96:ZZK6F7n5eRmDFJivohZFVB8
MD5:	76559278C9FE19A6BE09C4C9FDC77F5B
SHA1:	62F50171379E6A161B36B6115ADC84A87FEB8E34
SHA-256:	B039386EBB42D81235D5098E8E488E495FFA5B3DEF61DA999F190F710D9B0B81
SHA-512:	FC694110A71AD46B510D63AC8739C90FECF11B96E6E807E4653A41D905FBE242F40003515D9A0192FF17C851D20BE4D2E1E4994B643D2BA9C8826079BF9083C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^.....".... ....$.....@.....`.....l..$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data...;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.114412485087472
Encrypted:	false
SSDEEP:	12288:BZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:BZK6F7n5eRmDFJivohZFV
MD5:	7D0231DED93D4AB31C637F9BD2B87609
SHA1:	9D30B4333866D64D8F09B23BBC3D087B7FFB198B
SHA-256:	895A939E1E00FF74F0DA4FB66E7ACF9F4AB753352A7253A7501DF4D1A46F3A64
SHA-512:	737A92AF8AA0778215FA9FE5DED81F33E2DD852E8B684F688E49D008454BC0CAE0743195CFFD787A071A3011F125D09D729C2AC1DF75BB3B5B92CFC580B817 7
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....."..... .....$.....@.....`.....$..<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.640119387300135
Encrypted:	false
SSDEEP:	768:Sm6uxIL0DPeyQvEsNN6hU2hGGalaQkQcryUJU3fUrh6WeENiJDBPrxZt4W:p6MMD6hlBBjrywUKeWSDBPrxZaW
MD5:	A513A767CC9CC3E694D8C9D53B90B73E
SHA1:	F10B719117D26DAFCC9DBE54E9F9D78A0F80EE2A
SHA-256:	C9F7AC4322504D7EC8305973951A66FBE34E55E34A59409B5B574D627A474369
SHA-512:	03BBBC076D3497E35952143085B9DCC83EDE855A00A190F05712FC91F0C0C4301995D0123EBDCA75A59B93C51358EAD5C4030F8EE9C33F9D1BF1A0EDBC52FD 64
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.K.U.K.U.K.U.B..G.U.$.P.J.U.$.V.H.U.$.Q.Y.U.$.T.F.U.K.T...U .$.\.J.U.$...J.U.$.W.J.U.RichK.U.....PE..d...v.....".....n.....@6.....@.....`..... .....L.....F...p..... .....4....F..T.....@.....A.....text....-..... ..`.rdata..t....@.....2.....@..@.data.....`.....J.....@....pdata.....p..... ..L.....@..@.rsrc....F.....H...P.....@..@.reloc..4.....@..B..... .....

C:\Users\user\AppData\Local\OiZS\SLC.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.119868902164485
Encrypted:	false
SSDEEP:	12288:eZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw51:eZK6F7n5eRmDFJivohZFV51
MD5:	ADD63B02FC5977D9F0ADC80D62D9CBBB
SHA1:	F8395B176C5F9E52DD7274B783CA6523A2A88FA9
SHA-256:	8D62E1A88A477FECD4F4917D6C5CE3FC1B7D4B1B38658FA498761274657B2262
SHA-512:	F4AA611119D9BACE4DEBA5EFB8AFE439FE030A2F5ED2221F90CE773D896BFEC409E6B3CC44B89931A12139F04740668CC393E782EA57F021DF11C97DBB9675 B1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....."..... .....$.....@.....`.....3...$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\OiZS\msinfo32.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	370176
Entropy (8bit):	6.448503897594857
Encrypted:	false

SSDEEP:	6144:Uca2EiZg+uTUbSFWjSJiIOKZXcmg3GexhxiZEOHHrpm1XUZLxEZEOHHrpm1XUZLx:UB2PsUbSFWWAkZXcmkVx+tLpm1EwtLpr
MD5:	C471C6B06F47EA1C66E5FAA8DFCEF108
SHA1:	F8672A2B3B32956CBC948A954CEF236581045B78
SHA-256:	E2255751C1CF58596C8FE70C3093E099F8D71ED89580CFD0156FFCF0FED32861
SHA-512:	F7A2A31910CD4694B58FFCED83A2CCF633B5594859F178AFB9F67C02E3E664DA72701E7E45AA5590C4F1E1C99C82B665F0C0B80401506F0DFA49B61A8EEBD6E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....y...y...y..yz...y..y}...y..y\|...y..yx...y...x...y..yp...y..y....y..y{...y.Ri ch..y.....PE..d....a.....".....@.....0.....`..... .....$...h.....xJ.....(..... .. ...P...T.....P..... ....P... .....text..... ..`.rdata..H*.....,.....@..@.data....k...@.....(.....@....pdata..(.....D.....@..@.rsrc...xJ.....L...V..... ..@..@.reloc.. ....@..B..... .....

C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.069929843481676
Encrypted:	false
SSDEEP:	6144:NRq8Ez5tCqd6Nr6/TWeRhUz/vMNuEob69hbF1m0lpVGMD8i3ZdTgDt0kcRkdXgl6:NRquQ/TWeRhUz/vMNuEob69hBblHGu3t
MD5:	114A55D75AC7447F012B6D8EC8B1F7FC
SHA1:	37D5636D940D0A948000B94C84AD6C41162E593F
SHA-256:	E188143729B044955881302631BE577381B05B67E9899E09DB3573156719C70E
SHA-512:	446FD3024710E6994A0085CF3ADC0E395BE131898D7D932B383A19981C41637D27D9DABFB2177DBB62375CF4CCFC13722F5B828FF0FA9BB691F220A73D03558
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.m.Q.>.Q.>.Q.>.)E>.Q.>.5.?.Q.>.5.?.Q.>.Q.>+Q.>.5.?.Q.>.5.?.Q .>.5.?.Q.>.5)>.Q.>.5.?.Q.>Rich.Q.>.....PE..d...O.Uf.....".....(.....E.....@.....@.....e}..... .....8...\... .....x.....0..... T.....text...L..... ..`.imrsiv.....rdata..L.....@..@.data.....@....pda ta..x.....@..@.didat..x.....@....rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.114755158143574
Encrypted:	false
SSDEEP:	12288:8ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:8ZK6F7n5eRmDFJivohZFV
MD5:	20A8208130965F8A7BD5F9F5FC9E22AA
SHA1:	FC60176E08C12F95EF523B62231471FFBB427C1D
SHA-256:	6AE6C8AD8CE0153FE8DB30FD7E6B9B39DD1EDA7E0112A9579F535635264FBBA8
SHA-512:	AE802E08580C5BD2E3BF784BD959413F59A33F4FF79B56FC258C1381FEC34210B9A0A17E330F8ED8237B25EDD7CB388036A1A0E8DD3B83A6ABCE63282A1885 C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^.....".... ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows

Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.12207960232427
Encrypted:	false
SSDEEP:	12288:pZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:pZK6F7n5eRmDFJivohZFV
MD5:	C6770E4DA7DB91BE38365BE1E0BA6068
SHA1:	DC65AD3330C6DAB4BA88DA1A7CAFFBFE688E1EBC
SHA-256:	5BA0134390CB8218DC64CDA1AD7A12C0AF3A855DF57FB1D1623AAD39DC7E8CD4
SHA-512:	1B987FC1F594304BC733FF8E316D3D65A9380BD282BBDBF64BAB7FBC401387FAA7711B76D6E91CF9F8D26E9647BAE512AE31DDB098937A3598E9C9DE5ECFF4E0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....." ....$.....@.....`.....$...<.....0..(.....text..... .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	6.084247719186399
Encrypted:	false
SSDEEP:	12288:T9kJ4nbQXm4cVAyCSJLk1aciuMkTzOqUx6cl+RjJSzb0fK:T9k+N9CSJuah1cSqfC+RaYf
MD5:	2228E677678848E2FC693199947715E7
SHA1:	7AA34AC0938585EEFA9E0ABC80CCBD4E17651173
SHA-256:	9041F1AF7FD9A065B6C69D6CDF95F6FF939BF224C040816A0646540E145B73FF
SHA-512:	9B69EB763BC90FA8FE495FD1EA953276D68B8648737F209B98E777651AA89ABA4CE6449093B3E4C02B4350FF75AF508C05E6371D847279775993ABA04EFF950E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....].t...t...t.....t.....t.....t.....t.....t...t..gu.....t.....t.....t..Rich.t.....PE..d...c.]....."....@.....@.....u....`..... .....p....@...]...../.....@.....T.....`.....text..... ..`.rdata..N..... .....@..@.data.... .....@....pdata.../.....0.....@..@.rsrc....]...@...^.....@..@.reloc..@.....\.....@..B.....

C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.11595778237802
Encrypted:	false
SSDEEP:	12288:4ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:4ZK6F7n5eRmDFJivohZFV
MD5:	E8A052826532ACA1540ECDF8A5AB7B93
SHA1:	3E8C8AC80482188FC66D37AAA6AC1D5B4CE11F2A
SHA-256:	104DC24FB12A70B85E54725E60659481D8D6053BF3AB9F99EEFDCC6EE84F116A
SHA-512:	64729E52E776D75DB850E90D77300BC6813BC74649BB0878CBC93AFEC3BAB4E7835CB881E6266960324EB29B45F4886F380D8677BFBABCD6F4A1984E1A67480
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....." ....$.....@.....`.....+...$...<.....0..(.....text..... .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	5.729539450068024
Encrypted:	false
SSDEEP:	1536:8HSpBlnak9UH8bCAHZ1LQ434syPz7M5hh/kzhwS827HuYHwHugXEYJ6S7775MWUn:aC4HWCp/fM5hvNebgXEYJN73uWUZxtt
MD5:	9A68ADD12EB50DDE7586782C3EB9FF9C
SHA1:	2661E5F3562DD03C0ED21C33E2888E2FD1137D8C
SHA-256:	62A95C926C8513C9F3ACF65A5B33CBB88174555E2759C1B52DD6629F743A59ED
SHA-512:	156CAED6E1BF27B275E4BA0707FB550F1BF347A26361D6D3CAD12C612C327686950B47B6C5487110CF8B35A490FAADC812ADE3777FFF7ED76A528D970914A6E0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n.....Rich.....PE..d...U.E....."..... 2...R.....@*.....@.....8w....`.....8...8.....T.....T.....text..."1..... 2..... ..`.rdata..F....P.....6.....@..@.data.....@....pdata.....@..@.rsrc.....@..@.reloc..T.....t.....@..B.....

C:\Users\user\AppData\Local\Zc3\NETPLWIZ.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.114415103772413
Encrypted:	false
SSDEEP:	12288:pZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:pZK6F7n5eRmDFJivohZFV
MD5:	7EABC5F91F988A68D6FEFA888E7364D8
SHA1:	6A386985A20C69D439021E127B59E829D2B9AEBA
SHA-256:	90CB6CD5C15EF5E5B74345D839B04458C3FBAFEBCBF074618B7D37D5594693D4
SHA-512:	8F9B1365F2B9E242FE41F001002299EA3F6F979AD5984F4504201D1076A5CE04031BFBD782FA67FC0E2A3B3DE454E173B0019C4DB96D7C59E07580DB9B6C78D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....." ....$.....@.....`.....$...<.....0..(.....text..... .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\Zc3\Netplwiz.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.640119387300135
Encrypted:	false
SSDEEP:	768:Sm6uxIL0DPeyQvEsNN6hU2hGGalaQkQcryUJU3fUrh6WeENiJDBPrxZt4W:p6MMD6hlBBjrywUKeWSDBPrxZaW
MD5:	A513A767CC9CC3E694D8C9D53B90B73E
SHA1:	F10B719117D26DAFCC9DBE54E9F9D78A0F80EE2A
SHA-256:	C9F7AC4322504D7EC8305973951A66FBE34E55E34A59409B5B574D627A474369
SHA-512:	03BBBC076D3497E35952143085B9DCC83EDE855A00A190F05712FC91F0C0C4301995D0123EBDCA75A59B93C51358EAD5C4030F8EE9C33F9D1BF1A0EDBC52FD64
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.K.U.K.U.K.U.B..G.U.$.P.J.U.$.V.H.U.$.Q.Y.U.$.T.F.U.K.T...U.$.\.J.U.$...J.U.$.W.J.U.RichK.U.....PE..d...v....."..... n.....@6.....@.....`..... .....L.....F...p..... .....4....F..T.....@.....A.....text....-..... ..`.rdata..t....@.....2.....@..@.data.....`.....J.....@....pdata.....p..... ..L.....@..@.rsrc....F.....H...P.....@..@.reloc..4.....@..B.....

C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe

Process:	C:\Windows\explorer.exe

File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	111104
Entropy (8bit):	7.116157397823492
Encrypted:	false
SSDEEP:	3072:iFADqjCYMbEaznWfH22ZsuX2xKwMPTnaSrIrvDW:YAmCznWjZnXeKwMLnaqY
MD5:	25FA10F83BEDEF170C9BB47EE7E3CA91
SHA1:	FB271766DF5E14005CEE94916A013D34D81C820D
SHA-256:	AB09B14ED18D2874FDB191ECDA35DFC52BB6957E0E18B2F8F0F5209EE5D691D2
SHA-512:	62F8509CC29659220EBBD3AFF189E23B40120D3E81C434B4A640AB5D4EAEDE679C086433387459543B4E66DB0BB857ACC4A89B7963323E59E8D9C5583DED74E 1
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^...?...?...?...G...?...[...?...[...?...[...?...[...?...?...?...[...?...[~..?...[...?..Rich.?.....PE..d.....".....0.....7.....@.....`..... .....@M.,.....p[...p.....4...`G..T..... .....@.....A.....text.../.....0..... ..`.rdata..~....@.....4.....@..@.data.....`.....N.....@....pdata.....p.....P.....@..@.rsrc.. .p[.....\...T.....@..@.reloc..4.....@..B..... .....

C:\Users\user\AppData\Local\f3fc\appwiz.cpl

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.114621186933483
Encrypted:	false
SSDEEP:	12288:hZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:hZK6F7n5eRmDFJivohZFV
MD5:	9E8C33789ED70EEE47DD328431F2AE6E
SHA1:	1C244708EA0B2A020AEE71E206B249433C4BA6AB
SHA-256:	CEC661AF39B963161260F0F0966A44A56472E500919D067B043CF47E1049B5B1
SHA-512:	BA21E888C3376EA93F0E747961C2C555F6469B21FA7B2E7158033A72170B6492948C6E49D3F428FCD82D406D2DCF6601F0C1D68F61CC5734CEE6BC25D121C3F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^.....".... ....$.....@.....`.....'...$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1359872
Entropy (8bit):	5.141530810073766
Encrypted:	false
SSDEEP:	12288:oZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwi:oZK6F7n5eRmDFJivohZFVi
MD5:	243605D5386DF580F55C4E4D59E7B004
SHA1:	F04FCB0C64C02E7E3D4D0046A0AC0CCE98B0BD17
SHA-256:	0175443560F77D655BFF7F6864D0D7BE4BCD862ED901CB65E6242880924E7B35
SHA-512:	F08E146E694A44F9BAB88E45779E0BDA5BC6C18B7D560D592792100342C6999A2080572AC3018116CD6117B083FEB3E05DC090F4656A6ECAAD74847218C2D00
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^.....".... ....$.....@.....$...<.....0..(.....text..... .. ..@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\jOnYG\mfpmp.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	49688
Entropy (8bit):	6.083384253651048
Encrypted:	false
SSDEEP:	768:vcqpeHOwVxW4zmjjJF686T/5Lel2fBetjEWI9Whu3H1PcSP:vcEoVxJodg/tfiEAhu3VPcSP
MD5:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
SHA1:	F0C392891B6D73EADB20F669A29064910507E55E
SHA-256:	E459FF6CBA8C93589B206C07BDCCD2E6C57766BE6BB4754F2FB1DEF9EF2E3BDE
SHA-512:	6CFE325CD0A78D6ACC9473BA51069E234CB0F9A47F285A6204EE787902C77005491B41C301DD38602CC387329F214E700F9203E4ECE5077E58D30276821640E4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0._.Q`..Q`..Q`..)...Q`..5c..Q`..5d..Q`..Qa..Q`..5a..Q`..5e..Q `..5n..Q`..5...Q`..5b..Q`.Rich.Q`.....PE..d...^.A....."....R...V.....P).....@.....s....`..... .....h.....`.....$..... ....`z..T.....Pq.....`r.....H...`.....text....Q.....R..... ..`.rdata..T-...p.....V.....@..@.data.....@....pdata..... .....@..@.didat..0.....@....rsrc...`.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.127823609733136
Encrypted:	false
SSDEEP:	12288:JZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:JZK6F7n5eRmDFJivohZFV
MD5:	A0BC62657BA508B058ECEF8853308145
SHA1:	74423B4FE43B2504E461C5060D0C072C35B1D4A6
SHA-256:	8990FD02580ABCDD6F412EB85C665D00A90DDA4A8EAEF7223FC2732B504C5BAD
SHA-512:	F41CCD882DE0F3B73792941509EA091B18F1B3A12ADB6946CA942F29D8CA111092A5F53D0C0C306DEA169D94483F2D6790ACD3EB9D30E6742F03DBD064475E0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.:...}^....."..... .....$.....@.....`.....$...<.....0..(.....text.....  .. .....@.....  ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\p9w993CR\msra.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	600064
Entropy (8bit):	5.827796108757264
Encrypted:	false
SSDEEP:	6144:AXpiziCT8eKEnf3NyGO0Zc0q2097nxgw2KJUi1xfdkO6HCHJmDa+Yo0vZjqO:WkseKEf3YGO0iv2c72LlibdLl8a1om
MD5:	3240CC226FB8AC41A0431A8F3B9DD770
SHA1:	DD39C5B4E1BF3A66CB29940A246A771BEFF19A41
SHA-256:	62629BD91E153396CF990352A82A114FF9B3B264596CD846501D8BD55204B439
SHA-512:	86DF96691C564C1316278EFD3604566D4C9487D2C864B42C3036EC940CE736615CA6678B11B4C23BADABC9BC62643BADB331FEB2DC090839E721591C4464121
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....fx.h.+.h.+.h.+...*.h.+...*.h.+...*.h.+...*.h.+.h.+bi.+...*.h.+...+.h.+ ...*.h.+Rich.h.+.....PE..d...f)c....."....@.....`.....  .....8.....(...`.. (.....p..... ...T..... .....(...x...@.....text..... .. ..`.rdata...w.....x.....@..@.data...X....@.....  .....@....pdata..  (...`...*...*.....@..@.didat.....T..... ....@....rsrc...(.....V.....@..@.reloc.....p.....".....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	1450
Entropy (8bit):	7.34683669384493
Encrypted:	false
SSDEEP:	24:U+Z4dUAqtBVaDA9D0MdLWUguSvCej17jo4Lfif4cAqtmSX6KnGU:UW4dUnqA9Rd6UgZKe1jtfa0KnD
MD5:	673864A1D3C993C3265999B74A8BB7A6
SHA1:	322DE917A7FE9ABA6F0D011C021F51AE5DB732E0
SHA-256:	98024C541795E1071E8AE81A299E6A6CACF9010A7404F6F2C89B6AD0AB947BE4
SHA-512:	3F3C809E1EAA6373CD1D70A0C3A07E5EEC7D763120DB9E001070A1E0100FDCBA6830A93C5D3FBEFF8C366FA2603AA45E319721E75AF5CE741216756A1A7009A
Malicious:	false
Reputation:	unknown
Preview:	.....user.....RSA1.....zZ..M....@..E..y..`..b.5.....qH Y7..z..e.S....I.7m....'.....$..D..4..^.....C!..*.O.\o.a..,.....{...P.k~....$u.....N[...O.....z..O.....d..G...,c.R.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....@....A&s.Z.&..G..\....O<.W.52..... ....d+..Zb.Q.#...#...$.....@0nc.....+.;'...s.....@. .^....e.x.q...]..>..[..G):(I.X3.....=g.....6o..U.KR.....b.>e.....F.X&_..$..j.Ro..)..P...f!...1.V.tN*....r<..O...O....%.A...p..I..w6.i`..../.,.e.H..1....&.B.^)[1....L.q.[M.....?.... ..P..e.....Q\"I.-.8M...oc#..gr..C|.....w...%.WB3..&.]...ob..|c.:...$..F..W.$.....*.b...C..%....=..K..D...r.e.=..1..r....<.....c...._I..}.}..;.g...P.8...1x....>E..]4....&..va~.B.I...Z.....8...../s7..P.S.....M.. ....%..)O....1.%.....=.~F.....<..o.6N..R...hS8N}..j....j....?Q.{.X...Ao...w4.q.x.....;v...Zf_..L>..y..R*.Fs.....?3Q.1.B.g. I.=rnz.k..

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.127989624176249
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	IMqJSR2NIi.dll
File size:	1351680
MD5:	26c6fe63e7b7ddbbe73a97520ea5d93c
SHA1:	8787e8c20838eea270f4a1e11cf0da706ff610ad
SHA256:	9303d54f40b9c7f56d95a0aa39078f0878cab85d0b63e6f4b727749253013d8d
SHA512:	bd70c8df00cc74e83978cd958e53ca53d8b7a4908c6d673c33c090c7c76eee10a3264c70594d7380ab3ee811fff28511dde98314c9f58d9f42caa468294fe1d8
SSDEEP:	12288:qZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:qZK6F7n5eRmDFJivohZFV
File Content Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb.. (c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1400424b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E7D9D05 [Fri Mar 27 06:28:21 2020 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	4a2e61e1749a0183eccaadb9c4ef6ec2

Entrypoint Preview

Instruction
dec eax
mov dword ptr [00070639h], ecx
dec eax
lea ecx, dword ptr [FFFFF2F2h]
dec esp
mov dword ptr [0007064Bh], eax
dec esp
mov dword ptr [00070654h], edi
dec esp
mov dword ptr [00070655h], esi
dec eax
xor eax, eax
dec eax
inc eax
dec eax
add ecx, eax
dec esp
mov dword ptr [00070655h], esp
dec eax
dec ecx
dec eax
mov dword ptr [00070653h], esi
dec eax
test eax, eax
je 00007F1FBC65353Dh
dec eax
mov dword ptr [0007060Fh], esp
dec eax
mov dword ptr [00070600h], ebp
dec eax
mov dword ptr [00070649h], ebx
dec eax
mov dword ptr [0007063Ah], edi
dec eax
test eax, eax
je 00007F1FBC65351Ch
dec esp
mov dword ptr [000705FEh], ecx
dec esp
mov dword ptr [0007060Fh], ebp
dec eax
mov dword ptr [000705D0h], edx
jmp ecx
dec eax
add edi, ecx
retn 0008h
ud2
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push esi
dec eax
sub esp, 00000080h
dec eax
mov dword ptr [esp+78h], 58225FC8h
mov dword ptr [esp+60h], 2DFAE652h
mov al, byte ptr [esp+77h]
mov dl, al
add dl, FFFFFF85h
mov byte ptr [esp+77h], dl
mov word ptr [esp+5Eh], 3327h
dec esp
mov eax, dword ptr [esp+78h]
inc esp
mov ecx, dword ptr [esp+64h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x149010	0x20b	.dpewel
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9924	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xefc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x43000	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x418cc	0x42000	False	0.781412760417	data	7.78392111205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x66f43	0x67000	False	0.700320938258	data	7.87281050709	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xaa000	0x13ba7	0x14000	False	0.0782836914062	data	2.51707039551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0xbe000	0x138	0x1000	False	0.061279296875	PEX Binary Archive	0.599172422844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x69e	0x1000	False	0.123291015625	data	1.07831823765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xf31	0x1000	False	0.416748046875	data	5.36145191459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.vxl	0xc1000	0x14d4	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qwubgr	0xc3000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eer	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwwauf	0xc7000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pkc	0xc8000	0x42a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.npkda	0xc9000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vhs	0xca000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iaywj	0xcb000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nasi	0xcd000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zhvprh	0xce000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yatdsp	0xd5000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.njso	0xd6000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lgliat	0xd8000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ntqjh	0xd9000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sucsek	0xda000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qsxjui	0xdb000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.twctcm	0xdc000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nms	0xde000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ogj	0xdf000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vrkgb	0xe1000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gikfw	0xe2000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ktl	0xe3000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crcn	0xe4000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wtfr	0xe5000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hep	0xe6000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ywg	0xe7000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sqsp	0xe8000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gzb	0xe9000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fatlss	0xea000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.plqa	0xeb000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vzt	0xec000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dsbyd	0xed000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cdelc	0xef000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qkhkj	0xf0000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mnzegr	0xf1000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.krw	0xf2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jvsmn	0xf3000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bygpq	0xf4000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kzdbu	0xf6000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mwxorn	0xf7000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.raf	0xf8000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zcyw	0xf9000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zeczh	0xfa000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pvv	0xfc000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lug	0xfd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ski	0x143000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.japjd	0x144000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mwtzml	0x146000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vgssf	0x147000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qqb	0x148000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dpewel	0x149000	0x21b	0x1000	False	0.085693359375	data	1.06863909272	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbf0a0	0x2dc	data	English	United States
RT_MANIFEST	0xbf380	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	GetServiceDisplayNameW
KERNEL32.dll	LoadLibraryA, HeapUnlock

Exports

Name	Ordinal	Address
BrandingFormatString	1	0x14002a61c
BrandingFormatStringForEdition	2	0x140038d04
BrandingLoadBitmap	3	0x14001a9c0
BrandingLoadCursor	4	0x14001f07c
BrandingLoadIcon	5	0x14001b7a8
BrandingLoadImage	6	0x14000ef94
BrandingLoadNeutralStringForEdition	7	0x140013894
BrandingLoadString	8	0x140012140
BrandingLoadStringForEdition	9	0x140016c70
EulaFreeBuffer	10	0x140012220
GetEULAFile	11	0x140014c4c
GetEULAInCurrentUILanguage	12	0x14002f18c
GetHinstanceByNameSpace	13	0x140008444
GetInstalledEULAPath	14	0x140006c90
InstallEULA	15	0x14001aea4

Version Infos

Description	Data
LegalCopyright	Microsoft Corporation. All rights
InternalName	dpnhup
FileVersion	1.56
CompanyName	Microsoft C
ProductName	Sysinternals Streams
ProductVersion	6.1
FileDescription	Thai K
OriginalFilename	dpnhupnp.d
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map

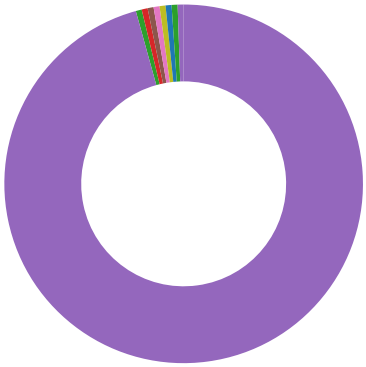
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- msra.exe
- msra.exe
- mfpmp.exe
- mfpmp.exe
- Netplwiz.exe
- Netplwiz.exe
- RecoveryDrive.exe
- RecoveryDrive.exe
- OptionalFeatures.exe
- OptionalFeatures.exe
- Netplwiz.exe
- Netplwiz.exe
- MusNotificationUx.exe
- MusNotificationUx.exe
- wscript.exe
- wscript.exe
- DevicePairingWizard.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6600**, Parent PID: **3104**

General	
Target ID:	0
Start time:	15:40:51
Start date:	23/03/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll"
Imagebase:	0x7ff7a0350000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.269553653.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6608**, Parent PID: **6600**

General

Target ID:	1
Start time:	15:40:52
Start date:	23/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll",#1
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: rundll32.exe PID: **6616**, Parent PID: **6600**

General

Target ID:	2
Start time:	15:40:52
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingFormatString
Imagebase:	0x7ff68e7e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.357465812.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IMqJSR2NIi.dll	unknown	1351680	success or wait	1	7FFFE24FF8D6	ReadFile

Analysis Process: rundll32.exe PID: **6628**, Parent PID: **6608**

General

Target ID:	3
Start time:	15:40:52
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\IMqJSR2NIi.dll",#1
Imagebase:	0x7ff68e7e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.248280628.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IMqJSR2NIi.dll	unknown	1351680	success or wait	1	7FFFE24FF8D6	ReadFile

Analysis Process: explorer.exe PID: **3616**, Parent PID: **6616**

General

Target ID:	5
Start time:	15:40:54
Start date:	23/03/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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\AppData\Roaming\Microsoft\Bibliography\Mm7ukttv	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\p9w993CR\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\p9w993CR\msra.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\jOnYG\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\jOnYG\mfpmp.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\ED1MV6ND\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\TQg3bhA\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\f3fc\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\f3fc\appwiz.cpl	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Zc3\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\Zc3\NETPLWIZ.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Zc3\Netplwiz.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\SxxDNr\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Sx xDNr\MusNotificationUx.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\XNPtE2qti\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\CdAVuX3\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Cd AVuX3\DevicePairingWizard.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\OiZS\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\OiZS\SLC.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\OiZS\msinfo32.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\p9w993CR\msra.exe	cannot delete	12	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	cannot delete	12	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\p9w993CR\msra.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\jOnYG\mfpmp.exe	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\jOnYG\mfpmp.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\f3fc\appwiz.cpl	cannot delete	4	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\f3fc\appwiz.cpl	success or wait	1	14005FB70	DeleteFileW

Copyright Joe Security LLC 2022

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Zc3\NETPLWIZ.dll	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Zc3\Netplwiz.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Zc3\NETPLWIZ.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Zc3\Netplwiz.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\SxxDNr\XmlLite.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll	cannot delete	12	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe	cannot delete	12	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\XNPtE2qti\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CdAVuX3\MFC42u.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\OiZS\msinfo32.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\OiZS\SLC.dll	success or wait	1	14005FB70	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	0	1355776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\p9w993CR\msra.exe	0	600064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\jOnYG\mfpmp.exe	0	49688	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe	0	39424	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe	0	877568	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe	0	111104	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Zc3\Netplwiz.exe	0	39424	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe	0	319488	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe	0	163840	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\CdAVuX3\DevicePairingWizard.exe	0	92160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\OiZS\msinfo32.exe	0	370176	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\xmllite.dll	unknown	227840	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\RMActivate_ssp.exe	unknown	492032	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wscript.exe	unknown	163840	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\version.dll	unknown	30568	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\dwm.exe	unknown	62464	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\verifier.exe	unknown	145920	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DevicePairingWizard.exe	unknown	92160	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\mfc42u.dll	unknown	1454592	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\xcopy.exe	unknown	47616	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DiskSnapshot.exe	unknown	91136	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\print.exe	unknown	16896	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\odbcad32.exe	unknown	73728	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\msinfo32.exe	unknown	370176	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\slc.dll	unknown	140800	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\dfrgui.exe	unknown	575488	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\drvinst.exe	unknown	166912	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\FXSUNATD.exe	unknown	19456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\omadmclient.exe	unknown	315904	success or wait	1	14005F8D6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{97835141-9F6F-84E8-FC95-D0A9D70CE65E}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{97835141-9F6F-84E8-FC95-D0A9D70CE65E}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{66992E05-6794-40A4-627E-DD68F796E8EC}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{66992E05-6794-40A4-627E-DD68F796E8EC}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6DC5B641-7D7D-AE80-F293-EFB97D288593}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6DC5B641-7D7D-AE80-F293-EFB97D288593}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98626F41-6CAC-503B-6510-86201EC6D80A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98626F41-6CAC-503B-6510-86201EC6D80A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0B020C7C-3556-8383-308C-89AF16C2DF7E}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0B020C7C-3556-8383-308C-89AF16C2DF7E}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D8BEBA22-F0F4-7E20-1C94-3F463061F968}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D8BEBA22-F0F4-7E20-1C94-3F463061F968}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B4B64980-5C49-54E1-46AF-706E53488BE8}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B4B64980-5C49-54E1-46AF-706E53488BE8}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C738A6DA-AFF8-9325-13C3-0F95BC02BBF6}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C738A6DA-AFF8-9325-13C3-0F95BC02BBF6}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{56C35E97-B633-CADA-6953-853774D64B65}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{56C35E97-B633-CADA-6953-853774D64B65}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E36B464D-98E8-D340-383B-E70855B47A51}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E36B464D-98E8-D340-383B-E70855B47A51}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{22F8CB54-2993-C7C6-5C95-E206609DB365}	success or wait	1	14006340A	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{22F8CB54-2993-C7C6-5C95-E206609DB365}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{38C2EDDF-4575-498E-CFC5-A025B7DCDE33}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{38C2EDDF-4575-498E-CFC5-A025B7DCDE33}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{102C0A7A-E3D6-05D5-B7D6-A8DA8D3ABA0D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{102C0A7A-E3D6-05D5-B7D6-A8DA8D3ABA0D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{378C8425-53B2-8145-74DD-4D5DF0DC2507}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{378C8425-53B2-8145-74DD-4D5DF0DC2507}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8A26C1BE-1F07-A383-1C5B-9F2363D75891}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8A26C1BE-1F07-A383-1C5B-9F2363D75891}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B07F962C-3013-57C5-6C47-FB7220E2A755}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B07F962C-3013-57C5-6C47-FB7220E2A755}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8A390866-C7E5-3A02-07C7-6DCCA74371B1}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8A390866-C7E5-3A02-07C7-6DCCA74371B1}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0D99E523-E4EE-96BD-9B7F-6216D09DE8A2}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0D99E523-E4EE-96BD-9B7F-6216D09DE8A2}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{22F8CB54-2993-C7C6-5C95-E206609DB365}\ShellFolder	{69EC23F8-AB5B-9B4A-34A7-D03F3AED6BB3}	binary	C9 13 27 05 6A 77 88 B3 B6 BC 1E 45 E9 CE 77 C5 0F A5 E8 07 28 A9 FC 74 0D DA 32 0F 92 C2 28 B9 73 8E 8A 00 95 A9 82 B2 39 1B AE 76 AC A6 37 8B 82 85 F4 FB F5 2C 2E 19 16 87 8C C9 23 7B 8A DD E2 BB C8 CE E4 C6 45	success or wait	1	140062470	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{56C35E97-B633-CADA-6953-853774D64B65}\ShellFolder	{2171A372-88D3-06A5-E18A-3E6E94E0F8C7}	binary	0A 60 67 CC 0C 5A 5E 83 DE 42 05 D3 91 28 DE F0 E6 50 DC 6A A4 FF BB 56 22 5B 3F 03 3B 09 67 6E 60 68 29 2C 26 0B F1 32 94 0A ED 7E 29 B5 C8 7E 5B D7 DD 44 BA 30 04 B7 8B 46 75 8C 29 9B 0E 01 3A E4 AC 65 EE 2B 5C 0C 54 BD CC EB FC FD 60 A9 FD 2C 44 FB 09 81 3D FC AD DF B1 A2	success or wait	1	140062470	RegSetValueExA

Analysis Process: rundll32.exe PID: **6768**, Parent PID: **6600**

General

Target ID:	7
Start time:	15:40:55
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingFormatStringForEdition
Imagebase:	0x7ff68e7e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.254908404.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security

Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IMqJSR2NIi.dll	unknown	1351680	success or wait	1	7FFFE24FF8D6	ReadFile

Analysis Process: rundll32.exe PID: **6932**, Parent PID: **6600**

General

Target ID:	9
Start time:	15:40:59
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\IMqJSR2NIi.dll,BrandingLoadBitmap
Imagebase:	0x7ff68e7e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000009.00000002.262721560.00007FFFE24A1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IMqJSR2NIi.dll	unknown	1351680	success or wait	1	7FFFE24FF8D6	ReadFile

Analysis Process: msra.exe PID: **6316**, Parent PID: **3616**

General

Target ID:	17
Start time:	15:41:46
Start date:	23/03/2022
Path:	C:\Windows\System32\msra.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msra.exe
Imagebase:	0x7ff69ab90000
File size:	600064 bytes
MD5 hash:	3240CC226FB8AC41A0431A8F3B9DD770
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msra.exe PID: **5220**, Parent PID: **3616**

General

Target ID:	19
Start time:	15:41:48
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\p9w993CR\msra.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\p9w993CR\msra.exe
Imagebase:	0x7ff7443c0000
File size:	600064 bytes
MD5 hash:	3240CC226FB8AC41A0431A8F3B9DD770
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000013.00000002.391467819.00007FFFEF951000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\p9w993CR\UxTheme.dll	unknown	1355776	success or wait	1	7FFFEF9AF8D6	ReadFile

Analysis Process: mfpmp.exe PID: 6676, Parent PID: 3616

General

Target ID:	20
Start time:	15:42:03
Start date:	23/03/2022
Path:	C:\Windows\System32\mfpmp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mfpmp.exe
Imagebase:	0x7ff69d120000
File size:	49688 bytes
MD5 hash:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mfpmp.exe PID: 6904, Parent PID: 3616

General

Target ID:	22
Start time:	15:42:05
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\jOnYG\mfpmp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\jOnYG\mfpmp.exe
Imagebase:	0x7ff7243d0000
File size:	49688 bytes
MD5 hash:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.426087810.00007FFFF6CD1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\jOnYG\MFPlat.DLL	unknown	1359872	success or wait	1	7FFFF6D2F8D6	ReadFile

Analysis Process: Netplwiz.exe PID: **7052**, Parent PID: **3616**

General	
Target ID:	25
Start time:	15:42:17
Start date:	23/03/2022
Path:	C:\Windows\System32\Netplwiz.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Netplwiz.exe
Imagebase:	0x7ff639280000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Netplwiz.exe PID: **7060**, Parent PID: **3616**

General	
Target ID:	26
Start time:	15:42:18
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\ED1MV6ND\Netplwiz.exe
Imagebase:	0x7ff6d63e0000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001A.00000002.454470944.00007FFFF6CD1000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\ED1MV6ND\NETPLWIZ.dll	unknown	1355776	success or wait	1	7FFFF6D2F8D6	ReadFile

Analysis Process: RecoveryDrive.exe PID: **5576**, Parent PID: **3616**

General	
Target ID:	28
Start time:	15:42:30
Start date:	23/03/2022
Path:	C:\Windows\System32\RecoveryDrive.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RecoveryDrive.exe
Imagebase:	0x7ff71d2d0000
File size:	877568 bytes
MD5 hash:	2228E677678848E2FC693199947715E7
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: RecoveryDrive.exe PID: **5760**, Parent PID: **3616**

General

Target ID:	29
Start time:	15:42:32
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\TQg3bhA\RecoveryDrive.exe
Imagebase:	0x7ff7f21c0000
File size:	877568 bytes
MD5 hash:	2228E677678848E2FC693199947715E7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001D.00000002.483809310.00007FFFF0DC1000.00000020.00000001.01000000.00000012.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\TQg3bhA\ReAgent.dll	unknown	1355776	success or wait	1	7FFFF0E1F8D6	ReadFile

Analysis Process: OptionalFeatures.exe PID: **3800**, Parent PID: **3616**

General

Target ID:	30
Start time:	15:42:44
Start date:	23/03/2022
Path:	C:\Windows\System32\OptionalFeatures.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\OptionalFeatures.exe
Imagebase:	0x7ff763e20000
File size:	111104 bytes
MD5 hash:	25FA10F83BEDEF170C9BB47EE7E3CA91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: OptionalFeatures.exe PID: **6096**, Parent PID: **3616**

General

Target ID:	31
Start time:	15:42:45
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\f3fc\OptionalFeatures.exe
Imagebase:	0x7ff7638d0000
File size:	111104 bytes
MD5 hash:	25FA10F83BEDEF170C9BB47EE7E3CA91
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001F.00000002.512496586.00007FFFF6CD1000.00000020.00000001.01000000.00000014.sdmp, Author: Joe Security

Analysis Process: Netplwiz.exe PID: **60**, Parent PID: **3616**

General	
Target ID:	32
Start time:	15:42:57
Start date:	23/03/2022
Path:	C:\Windows\System32\Netplwiz.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Netplwiz.exe
Imagebase:	0x7ff639280000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Netplwiz.exe PID: **3948**, Parent PID: **3616**

General	
Target ID:	33
Start time:	15:43:02
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\Zc3\Netplwiz.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Zc3\Netplwiz.exe
Imagebase:	0x7ff618290000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000021.00000002.548716546.00007FFFF6CD1000.00000020.00000001.01000000.00000016.sdmp, Author: Joe Security

Analysis Process: MusNotificationUx.exe PID: **2108**, Parent PID: **3616**

General	
Target ID:	36
Start time:	15:43:14
Start date:	23/03/2022
Path:	C:\Windows\System32\MusNotificationUx.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\MusNotificationUx.exe
Imagebase:	0x7ff77e360000
File size:	319488 bytes
MD5 hash:	114A55D75AC7447F012B6D8EC8B1F7FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MusNotificationUx.exe PID: **3600**, Parent PID: **3616**

General	
Target ID:	37
Start time:	15:43:16
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\SxxDNr\MusNotificationUx.exe
Imagebase:	0x7ff7e9950000
File size:	319488 bytes
MD5 hash:	114A55D75AC7447F012B6D8EC8B1F7FC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000025.00000002.579652462.00007FFFE3391000.00000020.00000001.01000000.00000019.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: wscript.exe PID: 4220, Parent PID: 3616

General	
Target ID:	39
Start time:	15:43:28
Start date:	23/03/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe
Imagebase:	0x7ff65aef0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 6152, Parent PID: 3616

General	
Target ID:	40
Start time:	15:43:30
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\XNPtE2qti\wscript.exe
Imagebase:	0x7ff775f70000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000028.00000002.611239452.00007FFFE3391000.00000020.00000001.01000000.0000001B.sdmp, Author: Joe Security

Analysis Process: DevicePairingWizard.exe PID: 4956, Parent PID: 3616

General	
Target ID:	41
Start time:	15:43:43

Start date:	23/03/2022
Path:	C:\Windows\System32\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DevicePairingWizard.exe
Imagebase:	0x7ff776ac0000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly

Copyright Joe Security LLC 2022