ID: 608207
Sample Name: x64.dll
Cookbook: default.jbs
Time: 21:44:07
Date: 12/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report x64.dll 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 6
System Summary 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
E-Banking Fraud 7
Persistence and Installation Behavior 7
Boot Survival 7
Hooking and other Techniques for Hiding and Protection 7
HIPS / PFW / Operating System Protection Evasion 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
World Map of Contacted IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
C:\Users\user\AppData\Local\Temp\Cjaq.cmd 13
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp 13
C:\Users\user\AppData\Local\Temp\NAmADA4.tmp 13
C:\Users\user\AppData\Local\Temp\tkcfGo.cmd 14
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a 14
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Wraljbotdtpzzk.lnk 14
C:\Users\user\AppData\Roaming\R3POs\wer.dll (copy) 15
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe 15
C:\Windows\System32\CCAL\MDMAppInstaller.exe 15
C:\Windows\system32\CCAL\WTSAPI32.dll (copy) 16
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17
Data Directories 18
Sections 18
Resources 19
Imports 20
Exports 20
Possible Origin 22
Network Behavior 22
Code Manipulations 22
User Modules 22
Hook Summary 22
Processes 22

Statistics 22
Behavior 22
System Behavior 23
Analysis Process: loaddll64.exePID: 7108, Parent PID: 3348 23
General 23
File Activities 23
Analysis Process: cmd.exePID: 7144, Parent PID: 7108 23
General 23
File Activities 24
Analysis Process: rundll32.exePID: 7152, Parent PID: 7108 24
General 24
File Activities 24
File Read 24
Analysis Process: rundll32.exePID: 7164, Parent PID: 7144 24
General 24
File Activities 25
File Read 25
Analysis Process: explorer.exePID: 684, Parent PID: 7152 25
General 25
File Activities 25
File Created 25
File Written 25
File Read 27
Registry Activities 27
Key Created 27
Key Value Created 28
Analysis Process: rundll32.exePID: 5980, Parent PID: 7108 29
General 29
File Activities 29
File Read 29
Analysis Process: rundll32.exePID: 5888, Parent PID: 7108 29
General 29
File Activities 30
File Read 30
Analysis Process: wermgr.exePID: 4784, Parent PID: 684 30
General 30
Analysis Process: cmd.exePID: 7136, Parent PID: 684 30
General 30
File Activities 30
File Created 30
File Moved 31
File Written 31
File Read 31
Analysis Process: conhost.exePID: 2928, Parent PID: 7136 31
General 31
Analysis Process: wermgr.exePID: 4176, Parent PID: 684 32
General 32
File Activities 32
File Read 32
Analysis Process: MDMAppInstaller.exePID: 2812, Parent PID: 684 32
General 32
Analysis Process: cmd.exePID: 5144, Parent PID: 684 32
General 32
File Activities 33
File Created 33
File Moved 33
File Written 33
File Read 33
Analysis Process: conhost.exePID: 4212, Parent PID: 5144 33
General 33
Analysis Process: wermgr.exePID: 5388, Parent PID: 684 34
General 34
File Activities 34
File Read 34
Analysis Process: schtasks.exePID: 4452, Parent PID: 684 34
General 34
File Activities 34
Analysis Process: conhost.exePID: 5560, Parent PID: 4452 35
General 35
Analysis Process: MDMAppInstaller.exePID: 5232, Parent PID: 1040 35
General 35
File Activities 35
File Read 35
Analysis Process: wermgr.exePID: 4164, Parent PID: 684 35
General 35
File Activities 36
File Read 36
Analysis Process: schtasks.exePID: 5080, Parent PID: 684 36
General 36
Analysis Process: conhost.exePID: 4788, Parent PID: 5080 36
General 36
Analysis Process: schtasks.exePID: 5500, Parent PID: 684 36
General 36
Analysis Process: conhost.exePID: 3464, Parent PID: 5500 37
General 37
Analysis Process: schtasks.exePID: 5744, Parent PID: 684 37
General 37
Analysis Process: conhost.exePID: 3488, Parent PID: 5744 37
General 37
Analysis Process: schtasks.exePID: 7092, Parent PID: 684 37
General 37
Analysis Process: conhost.exePID: 6756, Parent PID: 7092 38
General 38

Analysis Process: schtasks.exePID: 6344, Parent PID: 684 38
General 38
Analysis Process: conhost.exePID: 5188, Parent PID: 6344 38
General 38
Analysis Process: schtasks.exePID: 384, Parent PID: 684 39
General 39
Analysis Process: conhost.exePID: 3012, Parent PID: 384 39
General 39
Analysis Process: schtasks.exePID: 5228, Parent PID: 684 39
General 39
Analysis Process: conhost.exePID: 5220, Parent PID: 5228 39
General 39
Disassembly 40

Copyright Joe Security LLC 2022

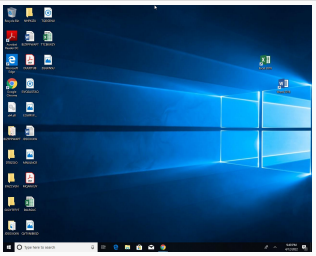
Windows Analysis Report

x64.dll

Overview

General Information

Sample Name:	x64.dll
Analysis ID:	608207
MD5:	66ac9a127ebb19..
SHA1:	b90e008f65d129..
SHA256:	94c0cedd61450d..
Tags:	64 exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

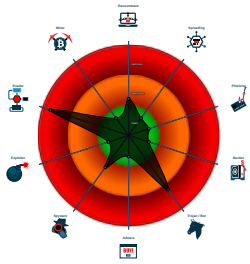
Dridex

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…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sigma detected: Suspicious Call by…
- Drops executables to the windows d…
- Uses schtasks.exe or at.exe to add…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7108 cmdline: loaddll64.exe "C:\Users\user\Desktop\x64.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7144 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\x64.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7164 cmdline: rundll32.exe "C:\Users\user\Desktop\x64.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7152 cmdline: rundll32.exe C:\Users\user\Desktop\x64.dll,IsInteractiveUserSession MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wermgr.exe (PID: 4784 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
      - cmd.exe (PID: 7136 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\Cjaq.cmd MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 2928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - wermgr.exe (PID: 4176 cmdline: "C:\Users\user\AppData\Roaming\R3POs\wermgr.exe" MD5: FF214585BF10206E21EA8EBA202FACFD)
      - MDMAppInstaller.exe (PID: 2812 cmdline: C:\Windows\system32\MDMAppInstaller.exe MD5: E2C777B6E3CE4C15C5657429A63787A3)
      - cmd.exe (PID: 5144 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\tkcfGo.cmd MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - wermgr.exe (PID: 5388 cmdline: "C:\Users\user\AppData\Roaming\R3POs\wermgr.exe" MD5: FF214585BF10206E21EA8EBA202FACFD)
      - schtasks.exe (PID: 4452 cmdline: "C:\Windows\System32\schtasks.exe" /Create /F /TN "Jvadjthzpd" /TR C:\Windows\system32\CCAL\MDMAppInstaller.exe /SC minute /MO 60 /RL highest MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - wermgr.exe (PID: 4164 cmdline: "C:\Users\user\AppData\Roaming\R3POs\wermgr.exe" MD5: FF214585BF10206E21EA8EBA202FACFD)
      - schtasks.exe (PID: 5080 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 4788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5500 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 3464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5744 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 3488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 7092 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6344 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 5188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 384 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 3012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5228 cmdline: schtasks.exe /Query /TN "Jvadjthzpd" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 5220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 5980 cmdline: rundll32.exe C:\Users\user\Desktop\x64.dll,QueryActiveSession MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 5888 cmdline: rundll32.exe C:\Users\user\Desktop\x64.dll,QueryUserToken MD5: 73C519F050C20580F8A62C849D49215A)
- MDMAppInstaller.exe (PID: 5232 cmdline: C:\Windows\system32\CCAL\MDMAppInstaller.exe MD5: E2C777B6E3CE4C15C5657429A63787A3)
- **cleanup**

Copyright Joe Security LLC 2022

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000021.00000002.611146050.0000000140001000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000006.00000002.421971716.0000000140001000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001F.00000002.604615787.0000000140001000.00000020.00000001.01000000.0000000E.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.435584389.0000000140001000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000018.00000002.622884365.0000000140001000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
31.2.MDMAppInstaller.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
33.2.wermgr.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
6.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 entries

Sigma Signatures

System Summary

Sigma detected: Suspicious Call by Ordinal

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

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

E-Banking Fraud

Yara detected Dridex unpacked file

Persistence and Installation Behavior

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

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

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)

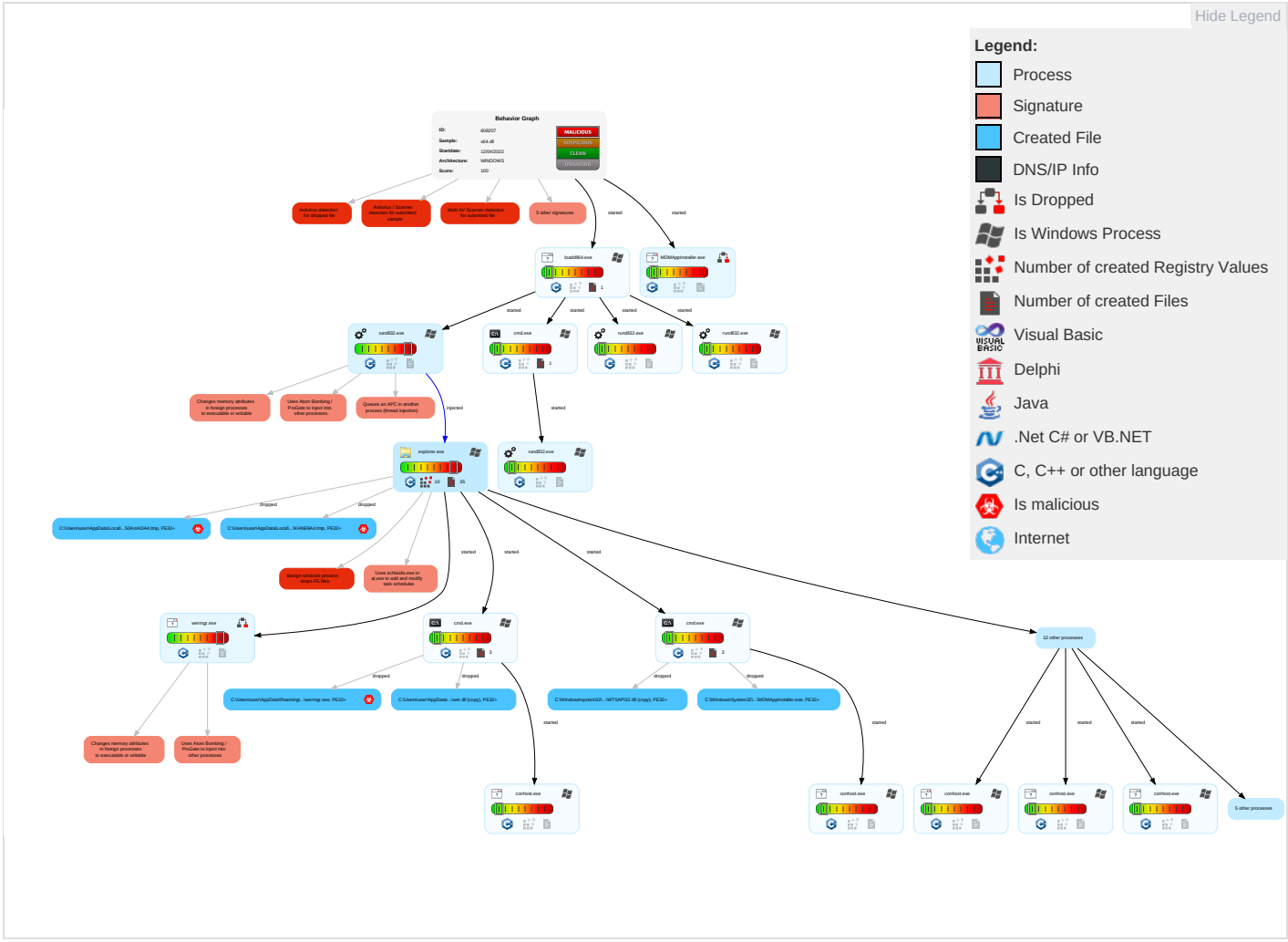
Uses Atom Bombing / ProGate to inject into other processes

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
1 Valid Accounts	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Valid Accounts	1 Valid Accounts	3 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	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)	1 Scheduled Task/Job	1 Windows Service	1 Timestomp	NTDS	2 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	1 Registry Run Keys / Startup Folder	3 1 2 Process Injection	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	1 Scheduled Task/Job	1 Rootkit	Cached Domain Credentials	2 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	1 Registry Run Keys / Startup Folder	1 2 1 Masquerading	DCSync	3 Process Discovery	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 Valid Accounts	Proc Filesystem	1 System Owner/User 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)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections 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)	3 1 2 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

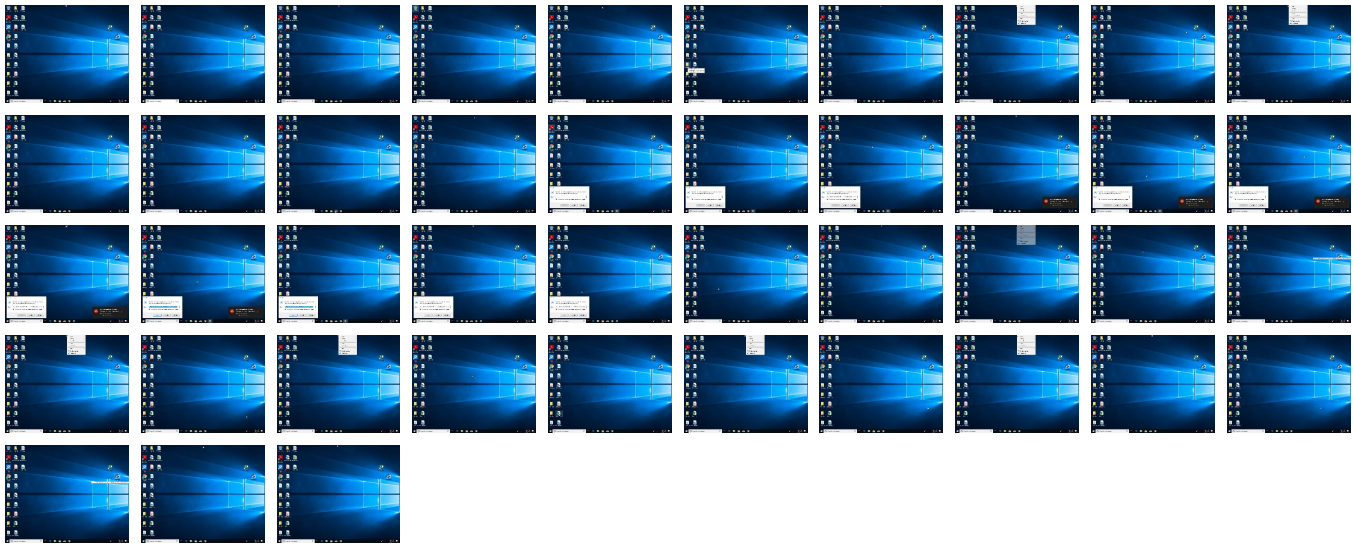
Behavior Graph



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
x64.dll	47%	Virustotal		Browse
x64.dll	37%	Metadefender		Browse
x64.dll	79%	ReversingLabs	Win64.Infostealer.Dridex	
x64.dll	100%	Avira	HEUR/AGEN.1207422	
x64.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\NAmADA4.tmp	100%	Avira	HEUR/AGEN.1207422	
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp	100%	Avira	HEUR/AGEN.1207422	
C:\Users\user\AppData\Local\Temp\NAmADA4.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	0%	ReversingLabs		
C:\Windows\System32\CCAL\MDMAppInstaller.exe	0%	Metadefender		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Windows\System32\CCAL\MDMAppInstaller.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.2.wermgr.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
31.2.MDMAppInstaller.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
28.2.wermgr.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
1.2.loaddll64.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
24.2.wermgr.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		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:	608207
Start date and time: 12/04/202221:44:07	2022-04-12 21:44:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	x64.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:	47
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
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@52/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.1% (good quality ratio 30.1%) • Quality average: 56.9% • Quality standard deviation: 39.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • 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, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, kv801.prod.do.dsp.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior 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 NtEnumerateKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:46:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Wraljbotdtpzzk C:\Users\user\AppData\Roaming\R3POs\wermgr.exe
21:46:25	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Wraljbotdtpzzk C:\Users\user\AppData\Roaming\R3POs\wermgr.exe
21:46:34	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Wraljbotdtpzzk.lnk
21:46:37	Task Scheduler	Run new task: Jvadjthzpd path: C:\Windows\system32\CCAL\MDMAppInstaller.exe

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\Temp\Cjaq.cmd

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	229
Entropy (8bit):	4.869685609305143
Encrypted:	false
SSDEEP:	6:8u5P9aZ51Me/N9aZ51d923f9X9aZ5IIpUQ:8u5sH1MueH1qGHnUQ
MD5:	03B3EA10D50CE5BB23379A28EA860902
SHA1:	8DC17B421435CA1D98D53F1586229D175F448F48
SHA-256:	0A3C5484A2F6190CFA103F7C4EB106C7F6C7E404B92780C3C0021E8EE9C5BEB5
SHA-512:	D60A16A86D863F97F2867E29AFA05887631D0E9ADAF2DF77E3B21B88E7EE36DC5B488ECCBC8A2F7D8D812BD8CB4B3188094A2B5E92148D781339152D345614 8
Malicious:	false
Preview:	md C:\Users\user\AppData\Roaming\R3POs..copy C:\Windows\system32\wermgr.exe C:\Users\user\AppData\Roaming\R3POs..move C:\Users\user\AppData\ Local\Temp\NAmADA4.tmp C:\Users\user\AppData\Roaming\R3POs\wer.dll..del %0 & exit

C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1064960
Entropy (8bit):	5.552014205230675
Encrypted:	false
SSDEEP:	12288:BabbKACcbDWwVexYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:MaXcfWwgmKrhncQYlez5nGa84djgol
MD5:	0DDBAA45951517107B9702E6CCC87906
SHA1:	370891865959F967B885A1EB9BFB459D73DF6105
SHA-256:	6C7F57824FA935D6BAB9ED7127A484F05433BB12FB6A5B9A6581B1173C5A237A
SHA-512:	421D4DCE4D4A521AA3CEC731D9FE1BE95A2510BB29B4493859EFEF6AF8816A4C274D261A349D23113A448A35F8AEBE1D3786788840DDB0D4DC5D2C7338F468 B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....x..j<.9<.9<.9?.t9l.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.l9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..l9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d....\.T....." .....f.....@..... .....@.....).&...`.....0.....h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Local\Temp\NAmADA4.tmp

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	5.550490003883871
Encrypted:	false
SSDEEP:	12288:UabbKACcbDWwVexYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:HaXcfWwgmKrhncQYlez5nGa84djgol
MD5:	6CB715AEF46D67EA68C59050D21B4522
SHA1:	F916645912DD962E8154073DF1AC4B707DFCC6D9
SHA-256:	EEE2DC41DA43B9601CB388825FC261C2FB0BBE60C7D3103574DE06CA694F01A1
SHA-512:	971829FD75C1917ED49CCFFD9990D7E6E77850B232BB34461C0BAA65F9B1A97E297BD797379CB46080E76038704994AFA3817874959D0426FD67130E782624E5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

Preview:	MZ.....@.....x..j<.9<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d....\.T......" .....f.....@..... .....P.....).&...`.....0..W...h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Local\Temp\tkcfGo.cmd

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	204
Entropy (8bit):	5.018347992860809
Encrypted:	false
SSDEEP:	6:8u5TAdXceTAJOXL4hAdd923f9bA8yTlJYxUQ:8u5MdXXXsudqFEVSxUQ
MD5:	60D9BF10F5BBC23ED46603A7E96335CD
SHA1:	56C387E5FBCBB2A4B8743C626155708018CC1015
SHA-256:	6CDF96C322D18F07F818C7BA846B1CEF9F907635A17733B59AFBFEB5589960E9
SHA-512:	2732D71724087D00EBB9EEAE5C4A7D3BA9D219E05768478F8676AAE5437B0670BF2272DCF53AF10F27C378C812E8BE34DF61793C477F5CA52B51A0326D5FC2AD
Malicious:	false
Preview:	md C:\Windows\system32\CCAL..copy C:\Windows\system32\MDMAppInstaller.exe C:\Windows\system32\CCAL..move C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp C:\Windows\system32\CCAL\WTSAPI32.dll..del %0 & exit

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	1451
Entropy (8bit):	7.327678216261483
Encrypted:	false
SSDEEP:	24:nqXB8+xVUlTbLZi1ecX4i1509VRLg45UkBg7avUGK55c/bXwlzPrXRXmA:nq++rUlTRi1NB15ub09kBqe7wlzjXRXv
MD5:	FB027688D1AE95BC43EFEBD156406E36
SHA1:	440623C7FB1DA9860CA2A0543D10B4168C87E28E
SHA-256:	9DC137B94E67305A9989FFA97AEEB98831D6931F19ACD0B67207344F756AA01A
SHA-512:	051CBD81738899F933441D62B3D42C679680023B38B1F5D5441DC747F8A44F64F4BC3400F5341D1533D8164D2D703DB9819623D3C479B9F4EC7543DC1AEA4CD
Malicious:	false
Preview:	.....user.....RSA1.....7....{.p..=.....qp.wi.....".L.gG.=.t!.s..e.....,...e....}.i._.M<.....\....<...EU$.m.....j..1K..... 4ukn....K..... .....z..O.....Y.A....W.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ... ...*n...*.b&.....Q..B...pcrlcQ*..... ....)1.....,*.x...>.t.....Hf/.....>...'..`f.....o....t.S....36...as3..'5.... ....L..{..5dE...b....aq...v.5._L..!.x6.?7N.6<H...0..e<mc.|%.....s.bl..11.....Z=....A.[.n.UG{.....[._..M..A.J.,I..).b.-%.oJ<.....I.=...x.....k..P.<4..e`L.(.....n.0.....NN...l.C.z..l.Kny. ....MnY.]p:%.b.4.....{N..f..{.X....0#..0...3..o.S3q5=M@...!..4.....%.8*0\|M ..h.l.....>..GM .a...,`.....,J.....%.c@.....u..Y..f...%...b....A0pz0.0...\&[.a#3.....)}...F...O..\.....Mv ....).....O.O,..Y...od].R.....j....$."..].dM...z.Lmd.."d..x...K0.eM.x."....r...Z.....q...o.D+...m.8H.&....?.Q.R+..K..t.x.....=.+...<

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Wraljbotdtpzzk.lnk

Process:	C:\Windows\explorer.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Apr 13 03:46:15 2022, mtime=Wed Apr 13 03:46:15 2022, atime=Wed Apr 11 22:34:22 2018, length=209312, window=hide
Category:	dropped
Size (bytes):	858
Entropy (8bit):	5.131205962827585
Encrypted:	false
SSDEEP:	12:8y8++Q4CNjyjCoscwY//W4xvuLkcF6j6QKtFS7DYjABmHdRsx2fd1Ucm:8yIOkFsc3u4xQAkxAqJm
MD5:	C69B35724D08B9AA7E320619F47BC2AA
SHA1:	D9D1E55F9B2D691085F36220C28813D8D4D772ED
SHA-256:	863FB90F0016B1B2BCAD15CA9C075B4BFAC36B86283E996C834C1E87C16DF77A
SHA-512:	443F6844FC5BBFE4FB861DD1998BE002448804E6F625A9EC29D6C0AB05F221204D2E3739F22D6759DD6C5D8647D5461631B52C6558DCEF13FB1E328C62ECC37
Malicious:	false
Preview:	L.....F.... ....0Rh.N...0Rh.N.....1.....:..DG..Yr?.D..U..k0.&...&.....-...my..3...=.h.N.....t...CFSF..1.....NM...AppData...t.Y^...H.g.3..(.....gVA.G..k...@. .....NM..T.%.....Y.....R..A.p.p.D.a.t.a...B.V.1.....T.%..Roaming.@.....NM..T.%.....Y.....s...R.o.a.m.i.n.g.....P.1.....T.%..R3POs.<.....T.%.T.%..... .....f.I.R.3.P.O.s.....`.2..1...LL. .wermgr.exe..F.....T.%.T.%.....t.....X..w.e.r.m.g.r...e.x.e....._.....-.....^.....q.....C:\Users\user\AppData\Roaming\R3POs \wermgr.exe.....\....\....\....\....\.R.3.P.O.s.\.w.e.r.m.g.r...e.x.e.`.....X.....computer..!a..%.H.VZAj.....s.....W...!a..%.H.VZAj.....s.....W..E.....9...1SPS..mD..pH .H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\R3POs\wer.dll (copy)	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	5.550490003883871
Encrypted:	false
SSDEEP:	12288:UabbKACcbDWwVexYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:HaXcfWwgmKrhncQYlez5nGa84djgol
MD5:	6CB715AEF46D67EA68C59050D21B4522
SHA1:	F916645912DD962E8154073DF1AC4B707DFCC6D9
SHA-256:	EEE2DC41DA43B9601CB388825FC261C2FB0BBE60C7D3103574DE06CA694F01A1
SHA-512:	971829FD75C1917ED49CCFFD9990D7E6E77850B232BB34461C0BAA65F9B1A97E297BD797379CB46080E76038704994AFA3817874959D0426FD67130E782624E5
Malicious:	false
Preview:	MZ.....@.....x..j<.9<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d....\.T....." .....f.....@..... .....P.....).&...`.....0..W...h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	209312
Entropy (8bit):	6.796289498157116
Encrypted:	false
SSDEEP:	6144:swTMBboFMSuc/9NPXWPJROo/wVJyB60OHyLC7vs:swTMB02SD/mXO64c2Hyw
MD5:	FF214585BF10206E21EA8EBA202FACFD
SHA1:	1ED4AE92D235497F62610078D51105C4634AFADE
SHA-256:	C48C430EB07ACC2FF8BDDD6057F5C9F72C2E83F67478F1E4A1792AF866711538
SHA-512:	24073F60B886C58F227769B2DD7D1439DF841784E43E753265DA761801FDA58FBEEDAC4A642E0A6ABDA40A6263153FAA1A9540DF6D35E38BF0EE5327EA55B4F E
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.Jl..jl..jl..c1...I...-..iI...-..qI..jI...H...-..mI...-..`I...-..KI...-..kI...-..kI..Rich jI.....PE..d...p....."....,.....`(.....@.....p.....`..... ..... ..0:.....!...`..\...@...T.....`Q..... `R.. ...t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@. .@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\...`.....@..B..... .....

C:\Windows\System32\CCAL\MDMAppInstaller.exe	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	145920
Entropy (8bit):	5.742854541048038
Encrypted:	false
SSDEEP:	3072:SfzsWjBQoVY9ZxvMlkD6F+UoOxsjlpfzX6:SfzsCBhy9dXUo+epfz
MD5:	E2C777B6E3CE4C15C5657429A63787A3
SHA1:	DFFC902982B618201D0DC46B91F1565DC7D04377
SHA-256:	7E02DBE7D9D4CE4DA15AD56123B0B9809F004F5C64917910BB55C8073DAA92B8
SHA-512:	2600F0CAE24C02DC64415E5A305AF7BB5B0CE97D9466F06D40430CFD03CE609A598BA10799E4D4A7EB7B1D95DD674F4E2522FA3767133786ED78FE5D7A2B3B 5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....OK7..*Y..*Y..*Y..*Y.dNZ..*Y.dN]..*Y.dN\..*Y.dNX.(*Y..*X..*Y.dNP..* Y.dN...*Y.dN[..*Y.Rich.*Y.....PE..d....$.6....."....@.....:.....@.....(....`..... .....@....`.....@..4.....p.....T..... .....R..(....Q.....8R.....H...@.....text...k>.....@..... ..`.rdata.....P.....D.....@..@.data...H....0.....@....pdata..4....@..... ....@..@.didat.....P.....@....rsrc.....`.....0.....@..@.reloc.....p.....8.....@..B..... .....

C:\Windows\system32\CCAL\WTSAPI32.dll (copy)	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1064960
Entropy (8bit):	5.552014205230675
Encrypted:	false
SSDEEP:	12288:BabbKACcbDWwVexYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:MaXcfWwgmKrhncQYlez5nGa84djgol
MD5:	0DDBAA45951517107B9702E6CCC87906
SHA1:	370891865959F967B885A1EB9BFB459D73DF6105
SHA-256:	6C7F57824FA935D6BAB9ED7127A484F05433BB12FB6A5B9A6581B1173C5A237A
SHA-512:	421D4DCE4D4A521AA3CEC731D9FE1BE95A2510BB29B4493859EFEF6AF8816A4C274D261A349D23113A448A35F8AEBE1D3786788840DDB0D4DC5D2C7338F468B
Malicious:	false
Preview:	MZ.....@.....x..j<.9<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9}.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d....\.T....." ....f.....@.....@.....).&...`.....0.....h...d.....(.....text....w..... ..`.rdata..... ..`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@...rsrc.....@..@.reloc...(.....0.....

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.568391526693222
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:	x64.dll
File size:	1060864
MD5:	66ac9a127ebb19f915987c31cf67d8d3
SHA1:	b90e008f65d129cd9ade9aa24a9e046d727ff3f6
SHA256:	94c0cedd61450d24b1195538edcd623b734749553680a42b5b64bc6194c2126a
SHA512:	ca0f1e93269456ab78e0ec00acc85310a30c7dfde9548b6898ba4694b1717ea2f3e09092431ffbf71431e8b9c7db04814b21fbef54f2a23f133c6a19f76717b8
SSDEEP:	12288:cabbKACcbDWwVexYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:faXcfWwgmKrhncQYlez5nGa84djgol
TLSH:	4D35CF4D492F1AC8D6A550F26B3387F6296EF4940420DEBD32B67025ED8DE7D8CC291B
File Content Preview:	MZ.....@.....x..j<..9<..9<..9?.t9I..9...8k..9S.49...9.ou9w..9...8M..9...82..9.7.9...91.I9u..9".:9...9'l590..9".=9/..9...8G..9R..8...9...8P..9S.39v..9?.u9i..9.7.9}..9...8...9".;9i..9..I9S..9Z.e9x..9?.w9...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x14002a5b0
Entrypoint Section:	.crt1
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x54B45CFA [Mon Jan 12 23:47:06 2015 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:	25c7ac00c91884fd2923a489ae9dfbca

Entrypoint Preview
Instruction
dec eax
mov dword ptr [00037CB9h], ecx
dec eax
mov dword ptr [00037CBAh], edx
dec eax
or dword ptr [00037CFBh], esi
dec eax
mov dword ptr [00037CFCh], edi
dec eax
mov dword ptr [00037CFDh], ebx
dec eax
mov dword ptr [00037CA6h], ebp
dec eax
mov dword ptr [00037CA7h], esp
dec esp
mov dword ptr [00037CA8h], eax
dec esp
mov dword ptr [00037CA9h], ecx
dec esp
mov dword ptr [00037CC2h], esp
dec esp
mov dword ptr [00037CB3h], ebp
dec esp
or dword ptr [00037CA4h], esi
dec esp
mov dword ptr [00037C95h], edi
dec eax
lea esi, dword ptr [FFFFD97Eh]
jmp esi
ud2
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x102010	0x8ee	.ncm
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ba68	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0xfc98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0x28bc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x610	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	0x2b000	0x90	.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	0x2779e	0x28000	False	0.761749267578	data	7.8179817907	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x29000	0xea5	0x1000	False	0.048095703125	data	0.477776163924	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.crt1	0x2a000	0x6fb	0x1000	False	0.25634765625	data	2.77764805072	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x2b000	0xcc0	0x1000	False	0.44921875	data	4.04304284558	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2c000	0x41e09	0x42000	False	0.577795780066	data	6.66561055311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x6e000	0xb46	0x1000	False	0.0595703125	data	0.53656064431	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
qwTG	0x6f000	0x2e9a2	0x2f000	False	0.818348986037	data	7.87184991211	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0xfc98	0x10000	False	0.223709106445	data	4.08759024615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0x28bc	0x3000	False	0.105550130208	data	5.14379878517	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.lqen	0xb1000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqb	0xf7000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gjd	0xf9000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wqhqlp	0xfb000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jriz	0xfd000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ebkl	0xff000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aoj	0x100000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ncm	0x102000	0x8fe	0x1000	False	0.253662109375	data	3.69309347361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0x9ee40	0x14a	data	English	United States
RT_STRING	0x9ef90	0x310	data	English	United States
RT_STRING	0x9f2a0	0x162	data	English	United States
RT_STRING	0x9f408	0x286	data	English	United States
RT_STRING	0x9f690	0x1cc	AmigaOS bitmap font	English	United States
RT_STRING	0x9f860	0x272	data	English	United States
RT_STRING	0x9fad8	0xee	data	English	United States
RT_STRING	0x9fbc8	0x144	data	English	United States
RT_STRING	0x9fd10	0xda	data	English	United States
RT_STRING	0x9fdf0	0x20e	data	English	United States
RT_STRING	0xa0000	0x326	data	English	United States
RT_STRING	0xa0328	0x33a	data	English	United States
RT_STRING	0xa0668	0x58c	data	English	United States
RT_STRING	0xa0bf8	0x2ca	data	English	United States
RT_STRING	0xa0ec8	0x2ce	data	English	United States
RT_STRING	0xa1198	0x3c6	data	English	United States
RT_STRING	0xa1560	0x41c	data	English	United States
RT_STRING	0xa1980	0x380	data	English	United States
RT_STRING	0xa1d00	0x408	data	English	United States
RT_STRING	0xa2108	0x4cc	data	English	United States
RT_STRING	0xa25d8	0x206	data	English	United States
RT_STRING	0xa27e0	0x50a	data	English	United States
RT_STRING	0xa2cf0	0x168	data	English	United States
RT_STRING	0xa2e58	0x12a	data	English	United States
RT_STRING	0xa2f88	0x36c	data	English	United States
RT_STRING	0xa32f8	0x2a8	data	English	United States
RT_STRING	0xa35a0	0x1de	data	English	United States
RT_STRING	0xa3780	0x3ec	data	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_STRING	0xa3b70	0x354	data	English	United States
RT_STRING	0xa3ec8	0x19c	data	English	United States
RT_STRING	0xa4068	0x27e	data	English	United States
RT_STRING	0xa42e8	0x3d8	data	English	United States
RT_STRING	0xa46c0	0x396	data	English	United States
RT_STRING	0xa4a58	0x336	data	English	United States
RT_STRING	0xa4d90	0x242	data	English	United States
RT_STRING	0xa4fd8	0x1ac	data	English	United States
RT_STRING	0xa5188	0x2f4	data	English	United States
RT_STRING	0xa5480	0x3ec	data	English	United States
RT_STRING	0xa5870	0x570	data	English	United States
RT_STRING	0xa5de0	0x3b2	Hitachi SH big-endian COFF object file, not stripped, 9472 sections, symbol offset=0x4b004200, 83895552 symbols, optional header size 12544	English	United States
RT_STRING	0xa6198	0x3aa	data	English	United States
RT_STRING	0xa6548	0x2c0	data	English	United States
RT_STRING	0xa6808	0x226	data	English	United States
RT_STRING	0xa6a30	0x248	data	English	United States
RT_STRING	0xa6c78	0x8f0	data	English	United States
RT_STRING	0xa7568	0x6aa	data	English	United States
RT_STRING	0xa7c18	0x456	data	English	United States
RT_STRING	0xa8070	0x522	data	English	United States
RT_STRING	0xa8598	0x51c	data	English	United States
RT_STRING	0xa8ab8	0x492	data	English	United States
RT_STRING	0xa8f50	0x432	data	English	United States
RT_STRING	0xa9388	0x6ec	data	English	United States
RT_STRING	0xa9a78	0x214	data	English	United States
RT_STRING	0xa9c90	0x472	AmigaOS bitmap font	English	United States
RT_STRING	0xaa108	0x3a2	data	English	United States
RT_STRING	0xaa4b0	0xb4	data	English	United States
RT_STRING	0xaa568	0x466	data	English	United States
RT_STRING	0xaa9d0	0x4b2	data	English	United States
RT_STRING	0xaae88	0x312	data	English	United States
RT_STRING	0xab1a0	0x106	data	English	United States
RT_STRING	0xab2a8	0x24e	data	English	United States
RT_STRING	0xab4f8	0x2b0	data	English	United States
RT_STRING	0xab7a8	0x392	data	English	United States
RT_STRING	0xabb40	0x34a	data	English	United States
RT_STRING	0xabe90	0x404	data	English	United States
RT_STRING	0xac298	0x3fc	data	English	United States
RT_STRING	0xac698	0x27a	data	English	United States
RT_STRING	0xac918	0xa8	data	English	United States
RT_STRING	0xac9c0	0xda	data	English	United States
RT_STRING	0xacaa0	0x2b2	data	English	United States
RT_STRING	0xacd58	0x274	data	English	United States
RT_STRING	0xacfd0	0x37c	data	English	United States
RT_STRING	0xad350	0x3fe	data	English	United States
RT_STRING	0xad750	0x2c0	data	English	United States
RT_STRING	0xada10	0x284	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetBinaryTypeW, GetModuleFileNameW, GetExitCodeProcess, GetModuleHandleW, GetCurrentProcess, GetCurrentProcessId, GetUserDefaultUILanguage
USER32.dll	SetProcessDefaultLayout, IsProcessDPIAware, ChildWindowFromPointEx, GetThreadDesktop
GDI32.dll	GetCharWidthW, FlattenPath
ADVAPI32.dll	InitiateSystemShutdownExW

Exports

Name	Ordinal	Address
IsInteractiveUserSession	1	0x140017388
QueryActiveSession	2	0x140026c6c
QueryUserToken	3	0x140004bc4
RegisterUsertokenForNoWinlogon	4	0x1400052fc
WTSCloseServer	5	0x14001e6dc
WTSConnectSessionA	6	0x140008eb8
WTSConnectSessionW	7	0x140011548
WTSCreateListenerA	8	0x140002340
WTSCreateListenerW	9	0x140017290
WTSDisconnectSession	10	0x140025978
WTSEnableChildSessions	11	0x14001e7b8
WTSEnumerateListenersA	12	0x140027d54
WTSEnumerateListenersW	13	0x140006740
WTSEnumerateProcessesA	14	0x140015468
WTSEnumerateProcessesExA	15	0x140001ccc
WTSEnumerateProcessesExW	16	0x1400283d0
WTSEnumerateProcessesW	17	0x140007568
WTSEnumerateServersA	18	0x14001faec
WTSEnumerateServersW	19	0x140016480
WTSEnumerateSessionsA	20	0x14000f194
WTSEnumerateSessionsExA	21	0x14001add4
WTSEnumerateSessionsExW	22	0x140010c34
WTSEnumerateSessionsW	23	0x140010830
WTSFreeMemory	24	0x1400079e8
WTSFreeMemoryExA	25	0x140001a10
WTSFreeMemoryExW	26	0x14000d420
WTSGetChildSessionId	27	0x140012468
WTSGetListenerSecurityA	28	0x14002160c
WTSGetListenerSecurityW	29	0x140022934
WTSIsChildSessionsEnabled	30	0x14000e2b4
WTSLogoffSession	31	0x140017848
WTSOpenServerA	32	0x14000d7b0
WTSOpenServerExA	33	0x140023da0
WTSOpenServerExW	34	0x140014938
WTSOpenServerW	35	0x14000b28c
WTSQueryListenerConfigA	36	0x14000adf4
WTSQueryListenerConfigW	37	0x140021de0
WTSQuerySessionInformationA	38	0x140026480
WTSQuerySessionInformationW	39	0x14000b01c
WTSQueryUserConfigA	40	0x14001ef04
WTSQueryUserConfigW	41	0x140018ee4
WTSQueryUserToken	42	0x1400161ac
WTSRegisterSessionNotification	43	0x1400247a8
WTSRegisterSessionNotificationEx	44	0x1400234c4
WTSSendMessageA	45	0x140011c24
WTSSendMessageW	46	0x140020f44
WTSSetListenerSecurityA	47	0x140019a50
WTSSetListenerSecurityW	48	0x1400010a8
WTSSetRenderHint	49	0x140019d14
WTSSetSessionInformationA	50	0x14000c4d4
WTSSetSessionInformationW	51	0x140002d30
WTSSetUserConfigA	52	0x140028434
WTSSetUserConfigW	53	0x140024668
WTSShutdownSystem	54	0x140016b6c
WTSStartRemoteControlSessionA	55	0x140008fc0
WTSStartRemoteControlSessionW	56	0x140010620
WTSStopRemoteControlSession	57	0x14001f8fc
WTSTerminateProcess	58	0x140004a04
WTSUnRegisterSessionNotification	59	0x1400135e0

Copyright Joe Security LLC 2022

Name	Ordinal	Address
WTSUnRegisterSessionNotificationEx	60	0x140002d0c
WTSVirtualChannelClose	61	0x140028138
WTSVirtualChannelOpen	62	0x14001f368
WTSVirtualChannelOpenEx	63	0x140003fbc
WTSVirtualChannelPurgeInput	64	0x140009418
WTSVirtualChannelPurgeOutput	65	0x1400088c4
WTSVirtualChannelQuery	66	0x1400214e4
WTSVirtualChannelRead	67	0x140002f3c
WTSVirtualChannelWrite	68	0x140013f94
WTSWaitSystemEvent	69	0x140004dac

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwSetEvent	INLINE	explorer.exe
RtlAllocateMemoryBlockLookaside	INLINE	explorer.exe
RtlAllocateMemoryZone	INLINE	explorer.exe
NtSetEvent	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: ntdll.dll

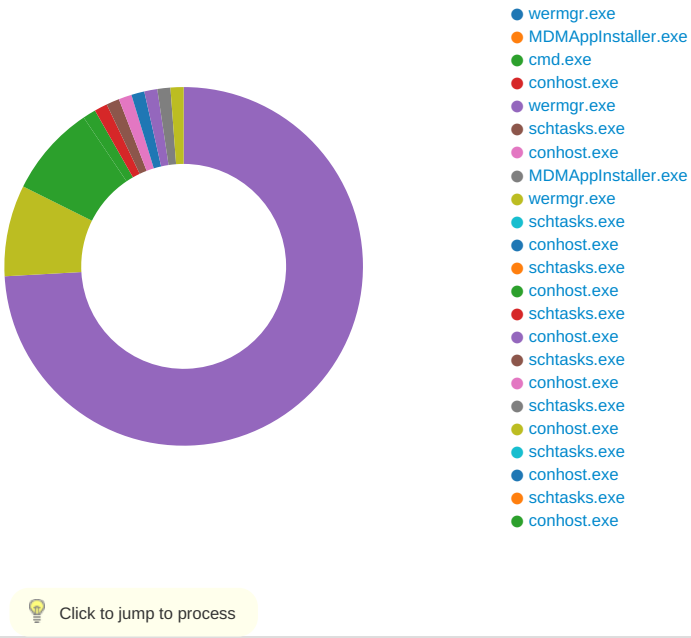
Function Name	Hook Type	New Data
ZwSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF
RtlAllocateMemoryBlockLookaside	INLINE	0x48 0x88 0x89 0x9E 0xE0 0x03
RtlAllocateMemoryZone	INLINE	0x8D 0xDA 0xAC 0xC2 0x24 0x49
NtSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- wermgr.exe
- cmd.exe
- conhost.exe

Copyright Joe Security LLC 2022



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 7108, Parent PID: 3348

General

Target ID:	1
Start time:	21:45:11
Start date:	12/04/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\x64.dll"
Imagebase:	0x7ff60a190000
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: 00000001.00000002.435584389.0000000140001000.00000020.00000001.01000000.00000003.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: 7144, Parent PID: 7108

General

Target ID:	2
Start time:	21:45:11
Start date:	12/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\x64.dll",#1

Imagebase:	0x7ff602050000
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: **7152**, Parent PID: **7108**

General

Target ID:	3
Start time:	21:45:12
Start date:	12/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\x64.dll,IsInteractiveUserSession
Imagebase:	0x7ff6d35e0000
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: 00000003.00000002.508980143.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\x64.dll	unknown	1060864	success or wait	1	140048F99	ReadFile

Analysis Process: rundll32.exe PID: **7164**, Parent PID: **7144**

General

Target ID:	4
Start time:	21:45:12
Start date:	12/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\x64.dll",#1
Imagebase:	0x7ff6d35e0000
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: 00000004.00000002.415891174.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\x64.dll	unknown	1060864	success or wait	1	140048F99	ReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **7152**

General

Target ID:	5
Start time:	21:45:14
Start date:	12/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
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\Local\Temp\NAmADA4.tmp	read attributes | synchronize | generic read	device | compressed	synchronous io non alert | non directory file	success or wait	1	14003E537	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\Cjaq.cmd	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	140048B94	CreateFileW
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp	read attributes | synchronize | generic read	device | compressed	synchronous io non alert | non directory file	success or wait	1	14003E537	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\tkcfGo.cmd	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	140048B94	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\NAmADA4.tmp	0	1069056	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 78 fd fd 6a 3c fd 39 3c fd 39 3c fd 39 3f fd 74 39 49 fd 39 95 fd 38 6b fd 39 53 fd 34 39 18 fd 39 fd 6f 75 39 77 fd 39 95 fd 38 4d fd 39 fd fd fd 38 32 fd 39 1b 37 fd 39 0f fd 39 31 fd 49 39 75 fd 39 22 fd 3a 39 13 fd 39 27 6c 35 39 30 fd 39 22 fd 3d 39 2f fd 39 fd fd fd 38 47 fd 39 52 fd fd 38 0c fd 39 95 fd 38 50 fd 39 53 fd 33 39 76 fd 39 3f fd 75 39 69 fd 39 1b 37 fd 39 7d fd 39 a8 fd 38 06 fd 39 22 fd 3b 39 69 fd 39 19 fd 49 39 53 fd 39 5a 1f 65 39 78 fd 39 3f fd 77 39 19 fd	MZ@xj<9<9<9?t9I98k9S499ou9w98M98297991I9u9":99'l5909"=9/98G9R898P9S39v9?u9i979}989";9i9I9S9Ze9x9?w9	success or wait	1	140049030	WriteFile
C:\Users\user\AppData\Local\Temp\Cjaq.cmd	0	229	6d 64 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 52 33 50 4f 73 0d 0a 63 6f 70 79 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 77 65 72 6d 67 72 2e 65 78 65 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 52 33 50 4f 73 0d 0a 6d 6f 76 65 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 4e 41 6d 41 44 41 34 2e 74 6d 70 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 52 33 50 4f 73 5c 77 65 72 2e 64 6c 6c 0d 0a 64 65 6c 20 25 30 20 26 20 65 78 69 74	md C:\Users\user\AppData\Roaming\R3POscopy C:\Windows\system32\wermgr.exe C:\Users\user\AppData\Roaming\R3POsmove C:\Users\user\AppData\Local\Temp\NAmADA4.tmp C:\Users\user\AppData\Roaming\R3POs\wer.dll del %0 & exit	success or wait	1	140049030	WriteFile
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp	0	1064960	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 78 fd fd 6a 3c fd 39 3c fd 39 3c fd 39 3f fd 74 39 49 fd 39 95 fd 38 6b fd 39 53 fd 34 39 18 fd 39 fd 6f 75 39 77 fd 39 95 fd 38 4d fd 39 fd fd fd 38 32 fd 39 1b 37 fd 39 0f fd 39 31 fd 49 39 75 fd 39 22 fd 3a 39 13 fd 39 27 6c 35 39 30 fd 39 22 fd 3d 39 2f fd 39 fd fd fd 38 47 fd 39 52 fd fd 38 0c fd 39 95 fd 38 50 fd 39 53 fd 33 39 76 fd 39 3f fd 75 39 69 fd 39 1b 37 fd 39 7d fd 39 a8 fd 38 06 fd 39 22 fd 3b 39 69 fd 39 19 fd 49 39 53 fd 39 5a 1f 65 39 78 fd 39 3f fd 77 39 19 fd	MZ@xj<9<9<9?t9I98k9S499ou9w98M98297991I9u9":99'l5909"=9/98G9R898P9S39v9?u9i979}989";9i9I9S9Ze9x9?w9	success or wait	1	140049030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tkcfGo.cmd	0	204	6d 64 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 43 43 41 4c 0d 0a 63 6f 70 79 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 4d 44 4d 41 70 70 49 6e 73 74 61 6c 6c 65 72 2e 65 78 65 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 43 43 41 4c 0d 0a 6d 6f 76 65 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 4b 48 4e 45 39 41 34 2e 74 6d 70 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 43 43 41 4c 5c 57 54 53 41 50 49 33 32 2e 64 6c 6c 0d 0a 64 65 6c 20 25 30 20 26 20 65 78 69 74	md C:\Windows\system32\CCALcopy C:\Windows\system32\MDMAppInstaller.exe C:\Windows\system32\CCALmove C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp C:\Windows\system32\CCAL\WTSAPI32.dlldel %0 & exit	success or wait	1	140049030	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\edpnotify.exe	unknown	59904	success or wait	1	140048F99	ReadFile
C:\Windows\System32\newdev.exe	unknown	71168	success or wait	1	140048F99	ReadFile
C:\Windows\System32\shutdown.exe	unknown	26624	success or wait	1	140048F99	ReadFile
C:\Windows\System32\fontdrvhost.exe	unknown	790304	success or wait	1	140048F99	ReadFile
C:\Windows\System32\winresume.exe	unknown	983008	success or wait	1	140048F99	ReadFile
C:\Windows\System32\wermgr.exe	unknown	209312	success or wait	1	140048F99	ReadFile
C:\Windows\System32\wer.dll	unknown	776888	success or wait	1	140048F99	ReadFile
C:\Windows\System32\LaunchWinApp.exe	unknown	41984	success or wait	1	140048F99	ReadFile
C:\Windows\System32\bootsect.exe	unknown	107416	success or wait	1	140048F99	ReadFile
C:\Windows\System32\dnscacheugc.exe	unknown	32256	success or wait	1	140048F99	ReadFile
C:\Windows\System32\MDMAppInstaller.exe	unknown	145920	success or wait	2	140048F99	ReadFile
C:\Windows\System32\wtsapi32.dll	unknown	64168	success or wait	1	140048F99	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{04FE2CBC-2242-CF5E-62B1-1E26A70419E5}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{04FE2CBC-2242-CF5E-62B1-1E26A70419E5}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B52FFDB6-386C-0961-A501-04F75F61E027}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B52FFDB6-386C-0961-A501-04F75F61E027}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABE33E08-EE35-EB02-2943-EF7CA5A2FBE5}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABE33E08-EE35-EB02-2943-EF7CA5A2FBE5}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{339155B0-19F1-282A-6E64-3D265FB6C24F}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{339155B0-19F1-282A-6E64-3D265FB6C24F}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DF0E200A-14F7-2870-3207-EE43A1D4402B}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DF0E200A-14F7-2870-3207-EE43A1D4402B}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E948FFB0-0294-5A09-9681-21FB05534FB0}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E948FFB0-0294-5A09-9681-21FB05534FB0}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9C6284E1-B038-049B-755D-7618733E96B8}	success or wait	1	140049B26	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9C6284E1-B038-049B-755D-7618733E96B8}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FEDF4965-F0A4-B260-EB46-6D913152C27C}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FEDF4965-F0A4-B260-EB46-6D913152C27C}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E61E1B2-47C8-4817-7403-CC2B94AD2568}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E61E1B2-47C8-4817-7403-CC2B94AD2568}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BC1C6CCD-930B-EE07-6DD0-AA7B96493757}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BC1C6CCD-930B-EE07-6DD0-AA7B96493757}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FBD54375-EC7C-1A9C-7CAF-44EE10C2528C}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FBD54375-EC7C-1A9C-7CAF-44EE10C2528C}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{43ECD239-4D6E-F56D-7DEE-9142FBB8E20B}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{43ECD239-4D6E-F56D-7DEE-9142FBB8E20B}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C3D17DFA-72D2-DD29-0120-83AAB1436071}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C3D17DFA-72D2-DD29-0120-83AAB1436071}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7BB8D77A-780A-F93D-74E5-03A29122D294}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7BB8D77A-780A-F93D-74E5-03A29122D294}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7EE66AD3-2DB0-0E26-DF62-F01F4FA18DAE}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7EE66AD3-2DB0-0E26-DF62-F01F4FA18DAE}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C8D925A8-4C87-E889-7CA5-E3D2B15B89AF}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C8D925A8-4C87-E889-7CA5-E3D2B15B89AF}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D8CC45C3-49BA-D15A-D535-D692F9CFA930}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D8CC45C3-49BA-D15A-D535-D692F9CFA930}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{54812D64-A07B-ABBA-C823-C554500F0AA1}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{54812D64-A07B-ABBA-C823-C554500F0AA1}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9C895F1A-3F2B-4358-571F-CE5C7F1F5F84}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9C895F1A-3F2B-4358-571F-CE5C7F1F5F84}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FBD54375-EC7C-1A9C-7CAF-44EE10C2528C}\ShellFolder	{C507D67E-696F-5FFD-DAC5-99B03B4F4508}	binary	5F 50 BF 84 A7 1C 06 50 2F 66 A8 43 66 9B F6 8A C9 3A 66 28 F3 C4 40 9E C5 92 57 7E BF 13 67 D8 C9 4B 2A 7D 61 77 53 8F D1 3A 9C 90 C1 2B 47 AD 58 57 9A F2 51 26 C2 62 69 6F 61 6B 7A 40 5E BF C7 48 4E 16 A7 A4 26 1C 92 1B	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E61E1B2-47C8-4817-7403-CC2B94AD2568}\ShellFolder	{B1948CD1-9E47-9076-D9B7-C38664E5494A}	binary	E8 C1 E6 8F 45 EC FE B9 D5 01 16 87 93 6A 6F 65 47 9B 88 E1 41 4C 26 F7 96 AA 91 E5 79 5A E5 ED 37 A8 60 FD 9F 37 C6 8A A2 EB E2 B2 FC 61 7F 74 B1 F7 DC D4 68 CE D2 12 85 35 CC 8A CD 46 8F EF 56 8A 4E 52 94 74 1A 4C D3 E2 67 59 7C EE 92 CA 01 10 BD BC 20 F8 1A 75 69 75 F2 55 A7	success or wait	1	14004A977	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E61E1B2-47C8-4817-7403-CC2B94AD2568}\ShellFolder	{DBE3B650-C156-7834-F96A-FAD4C6C1BF9C}	binary	91 F1 5B E4 B2 07 FE AF 34 33 E3 10 1C A3 A1 0D CF F2 9A 94 0A 34 AD 5D 01 49 11 06 0F 8D 9A 4A 81 98 4F 36 4C 06 D0 ED F4 0F B1 64 95 70 E8 7F AC 19 62 D2 B3 A8 FE B2 93 7E 90 70 EB 4D 8B 94 D0 9A F9 CF BE 12 AD C3 36 CE 69 30 A8 45 DC 7D 8F 70 F6 29 03 10 E8 B0 03 BA C3 21 39 0B 74 4B D0 B5	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Wraljbotdtpzzk	unicode	C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E61E1B2-47C8-4817-7403-CC2B94AD2568}\ShellFolder	{0938A86E-AC12-626A-4207-D6B1D1BFC8E8}	binary	BD 67 AB F4 CC 6E 8F 1A D8 8A 85 97 EC CF AE A1 6B DB 81 27 D4 A0 DB 81 FE F2 47 6E 57 7D 0D 6B E6 4D 82 D6 BC FD 3B 8F 22 B5 E3 AD 67 2D 19 BD 9A 43 6E CC F5 E2 20 D6 04 B5 22 F8 A9 D7 9F F9 88 90 32 CE 22 5D E1 43 1A 19 BA D5 CD FD D9 83 C9 7A B1 26 3C 9E 31 EE 6C 9F 8A 01 E7 F0 10 EB BE 4E A6 B1 DE 8F	success or wait	1	14004A977	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5980**, Parent PID: **7108**

General

Target ID:	6
Start time:	21:45:15
Start date:	12/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\x64.dll,QueryActiveSession
Imagebase:	0x7ff6d35e0000
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: 00000006.00000002.421971716.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\x64.dll	unknown	1060864	success or wait	1	140048F99	ReadFile

Analysis Process: rundll32.exe PID: **5888**, Parent PID: **7108**

General

Target ID:	8
Start time:	21:45:19
Start date:	12/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\x64.dll,QueryUserToken
Imagebase:	0x7ff6d35e0000
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: 00000008.00000002.429395051.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\x64.dll	unknown	1060864	success or wait	1	140048F99	ReadFile

Analysis Process: wermgr.exe PID: 4784, Parent PID: 684

General

Target ID:	16
Start time:	21:46:11
Start date:	12/04/2022
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff6bd590000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 7136, Parent PID: 684

General

Target ID:	17
Start time:	21:46:13
Start date:	12/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\Cjaq.cmd
Imagebase:	0x7ff602050000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\R3POs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF60205A1B5	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF6020558E5	CopyFileExW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\NAmADA4.tmp	C:\Users\user\AppData\Roaming\R3POs\wer.dll	success or wait	1	7FF602066058	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\R3POs\wermgr.exe	0	131072	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2e 28 6a fd 6a 49 04 fd 6a 49 04 fd 6a 49 04 fd 63 31 fd fd 0e 49 04 fd 05 2d 07 fd 69 49 04 fd 05 2d 00 fd 71 49 04 fd 6a 49 05 fd 0b 48 04 fd 05 2d 05 fd 6d 49 04 fd 05 2d 01 fd 60 49 04 fd 05 2d 0c fd 4b 49 04 fd 05 2d fd fd 6b 49 04 fd 05 2d 06 fd 6b 49 04 fd 52 69 63 68 6a 49 04 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 70 fd 67 00 00 00	MZ@!L!This program cannot be run in DOS mode.$.(jIjIjIc1I-iI-qIjIH-mI-`I-KI-kI-kIRichjIPEdp	success or wait	2	7FF6020558E5	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cjaq.cmd	unknown	8191	success or wait	4	7FF60205F404	ReadFile
C:\Windows\System32\wermgr.exe	unknown	512	success or wait	1	7FF602056290	ReadFile
C:\Users\user\AppData\Local\Temp\Cjaq.cmd	unknown	8191	end of file	1	7FF60205F404	ReadFile

Analysis Process: conhost.exe PID: **2928**, Parent PID: **7136**

General

Target ID:	20
Start time:	21:46:14
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Reputation:	high

Analysis Process: wermgr.exe PID: 4176, Parent PID: 684

General

Target ID:	24
Start time:	21:46:25
Start date:	12/04/2022
Path:	C:\Users\user\AppData\Roaming\R3POs\wermgr.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\R3POs\wermgr.exe"
Imagebase:	0x7ff7e4380000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
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: 00000018.00000002.622884365.0000000140001000.00000020.00000001.01000000.0000000C.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\Roaming\R3POs\wer.dll	unknown	1069056	success or wait	1	140048F99	ReadFile

Analysis Process: MDMAppInstaller.exe PID: 2812, Parent PID: 684

General

Target ID:	25
Start time:	21:46:26
Start date:	12/04/2022
Path:	C:\Windows\System32\MDMAppInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\MDMAppInstaller.exe
Imagebase:	0x7ff7b4780000
File size:	145920 bytes
MD5 hash:	E2C777B6E3CE4C15C5657429A63787A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5144, Parent PID: 684

General

Target ID:	26
Start time:	21:46:31
Start date:	12/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\tkcfGo.cmd
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\CCAL	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF60205A1B5	CreateDirectoryW
C:\Windows\system32\CCAL\MDMAppInstaller.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF6020558E5	CopyFileExW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\KHNE9A4.tmp	C:\Windows\system32\CCAL\WTSAPI32.dll	success or wait	1	7FF602066058	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\CCAL\MDMAppInstaller.exe	0	131072	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f 4b 37 fd 0b 2a 59 fd 0b 2a 59 fd 0b 2a 59 fd 64 4e 5a fd 08 2a 59 fd 64 4e 5d fd 1d 2a 59 fd 64 4e 5c fd 01 2a 59 fd 64 4e 58 fd 28 2a 59 fd 0b 2a 58 fd fd 2a 59 fd 64 4e 50 fd 06 2a 59 fd 64 4e fd fd 0a 2a 59 fd 64 4e 5b fd 0a 2a 59 fd 52 69 63 68 0b 2a 59 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd 24 fd 36 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 0c 00 40 01	MZ@!L!This program cannot be run in DOS mode.$OK7*Y*Y*YdNZ*Y dN]*YdN*YdNX(*Y*X*YdNP*YdN*Yd N[*YRich*YPEd$6"@	success or wait	2	7FF6020558E5	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tkcfGo.cmd	unknown	8191	success or wait	4	7FF60205F404	ReadFile
C:\Windows\System32\MDMAppInstaller.exe	unknown	512	success or wait	1	7FF602056290	ReadFile
C:\Users\user\AppData\Local\Temp\tkcfGo.cmd	unknown	8191	end of file	1	7FF60205F404	ReadFile

Analysis Process: conhost.exe PID: **4212**, Parent PID: **5144**

General

Target ID:	27
Start time:	21:46:32
Start date:	12/04/2022

Copyright Joe Security LLC 2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: **5388**, Parent PID: **684**

General

Target ID:	28
Start time:	21:46:34
Start date:	12/04/2022
Path:	C:\Users\user\AppData\Roaming\R3POs\wermgr.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\R3POs\wermgr.exe"
Imagebase:	0x7ff7e4380000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
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: 0000001C.00000002.595393684.0000000140001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\R3POs\wer.dll	unknown	1069056	success or wait	1	140048F99	ReadFile

Analysis Process: schtasks.exe PID: **4452**, Parent PID: **684**

General

Target ID:	29
Start time:	21:46:34
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /F /TN "Jvadjthzpd" /TR C:\Windows\system32\CCAL\MDMAppInstaller.exe /SC minute /MO 60 /RL highest
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5560**, Parent PID: **4452**

General	
Target ID:	30
Start time:	21:46:36
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MDMAppInstaller.exe PID: **5232**, Parent PID: **1040**

General	
Target ID:	31
Start time:	21:46:37
Start date:	12/04/2022
Path:	C:\Windows\System32\CCAL\MDMAppInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\CCAL\MDMAppInstaller.exe
Imagebase:	0x7ff6c5240000
File size:	145920 bytes
MD5 hash:	E2C777B6E3CE4C15C5657429A63787A3
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: 0000001F.00000002.604615787.0000000140001000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\CCAL\WTSAPI32.dll	unknown	1064960	success or wait	1	140048F99	ReadFile

Analysis Process: wermgr.exe PID: **4164**, Parent PID: **684**

General	
Target ID:	33
Start time:	21:46:43
Start date:	12/04/2022
Path:	C:\Users\user\AppData\Roaming\R3POs\wermgr.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\R3POs\wermgr.exe"
Imagebase:	0x7ff7e4380000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
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: 00000021.00000002.611146050.0000000140001000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\R3POs\wer.dll	unknown	1069056	success or wait	1	140048F99	ReadFile

Analysis Process: schtasks.exe PID: **5080**, Parent PID: **684**

General

Target ID:	34
Start time:	21:46:56
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4788**, Parent PID: **5080**

General

Target ID:	35
Start time:	21:46:57
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5500**, Parent PID: **684**

General

Target ID:	36
Start time:	21:47:20
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Analysis Process: conhost.exe PID: **3464**, Parent PID: **5500**

General	
Target ID:	37
Start time:	21:47:21
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5744**, Parent PID: **684**

General	
Target ID:	38
Start time:	21:47:42
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3488**, Parent PID: **5744**

General	
Target ID:	39
Start time:	21:47:43
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **7092**, Parent PID: **684**

General	
Target ID:	40
Start time:	21:48:04
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe

Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6756**, Parent PID: **7092**

General	
Target ID:	41
Start time:	21:48:05
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6344**, Parent PID: **684**

General	
Target ID:	42
Start time:	21:48:26
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5188**, Parent PID: **6344**

General	
Target ID:	43
Start time:	21:48:26
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **384**, Parent PID: **684**

General	
Target ID:	44
Start time:	21:48:47
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3012**, Parent PID: **384**

General	
Target ID:	45
Start time:	21:48:48
Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5228**, Parent PID: **684**

General	
Target ID:	46
Start time:	21:49:09
Start date:	12/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /Query /TN "Jvadjthzpd"
Imagebase:	0x7ff701990000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5220**, Parent PID: **5228**

General	
Target ID:	47
Start time:	21:49:09

Start date:	12/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly