ID: 492853
Sample Name: A2qAaSVuU2
Cookbook: default.jbs
Time: 03:36:37
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Windows Analysis Report A2qAaSVuU2

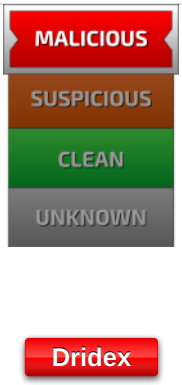
Overview

General Information

Sample Name:	A2qAaSVuU2 (renamed file extension from none to dll)
Analysis ID:	492853
MD5:	f8295446e335b67.
SHA1:	18b9a40791f1a52.
SHA256:	96705595655fd81.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:

Detection

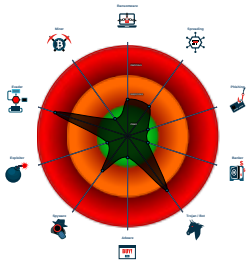


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 samp…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Contains functionality to automate e…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 3104 cmdline: loaddll64.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 5772 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3332 cmdline: rundll32.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2588 cmdline: rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxFreeMemory MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - SysResetErr.exe (PID: 2876 cmdline: C:\Windows\system32\SysResetErr.exe MD5: 6A3F2F3C36FE45A87E3BFA80B6D92E07)
      - SysResetErr.exe (PID: 484 cmdline: C:\Users\user\AppData\Local\AxQmthi0\SysResetErr.exe MD5: 6A3F2F3C36FE45A87E3BFA80B6D92E07)
      - RecoveryDrive.exe (PID: 5932 cmdline: C:\Windows\system32\RecoveryDrive.exe MD5: 2228E677678848E2FC693199947715E7)
      - RecoveryDrive.exe (PID: 6092 cmdline: C:\Users\user\AppData\Local\A1gpxNou\RecoveryDrive.exe MD5: 2228E677678848E2FC693199947715E7)
      - MusNotificationUx.exe (PID: 4756 cmdline: C:\Windows\system32\MusNotificationUx.exe MD5: 114A55D75AC7447F012B6D8EC8B1F7FC)
      - MusNotificationUx.exe (PID: 3940 cmdline: C:\Users\user\AppData\Local\FQTqHJ\MusNotificationUx.exe MD5: 114A55D75AC7447F012B6D8EC8B1F7FC)
      - SndVol.exe (PID: 3532 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - SndVol.exe (PID: 1208 cmdline: C:\Users\user\AppData\Local\QiP6c\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - EhStorAuthn.exe (PID: 3016 cmdline: C:\Windows\system32\EhStorAuthn.exe MD5: 5B9BB7B6DD9A81D42F057BA252DC3B63)
      - EhStorAuthn.exe (PID: 2424 cmdline: C:\Users\user\AppData\Local\r1aQ\EhStorAuthn.exe MD5: 5B9BB7B6DD9A81D42F057BA252DC3B63)
      - mstsc.exe (PID: 5972 cmdline: C:\Windows\system32\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
      - mstsc.exe (PID: 5668 cmdline: C:\Users\user\AppData\Local\VgY\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
  - rundll32.exe (PID: 2436 cmdline: rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxNewJob MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 800 cmdline: rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxNewJobEx MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000015.00000002.387213363.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000029.00000002.529730818.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.339300443.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.274418377.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000022.00000002.470825407.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

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 automate explorer (e.g. start an application)

Uses Atom Bombing / ProGate to inject into other processes

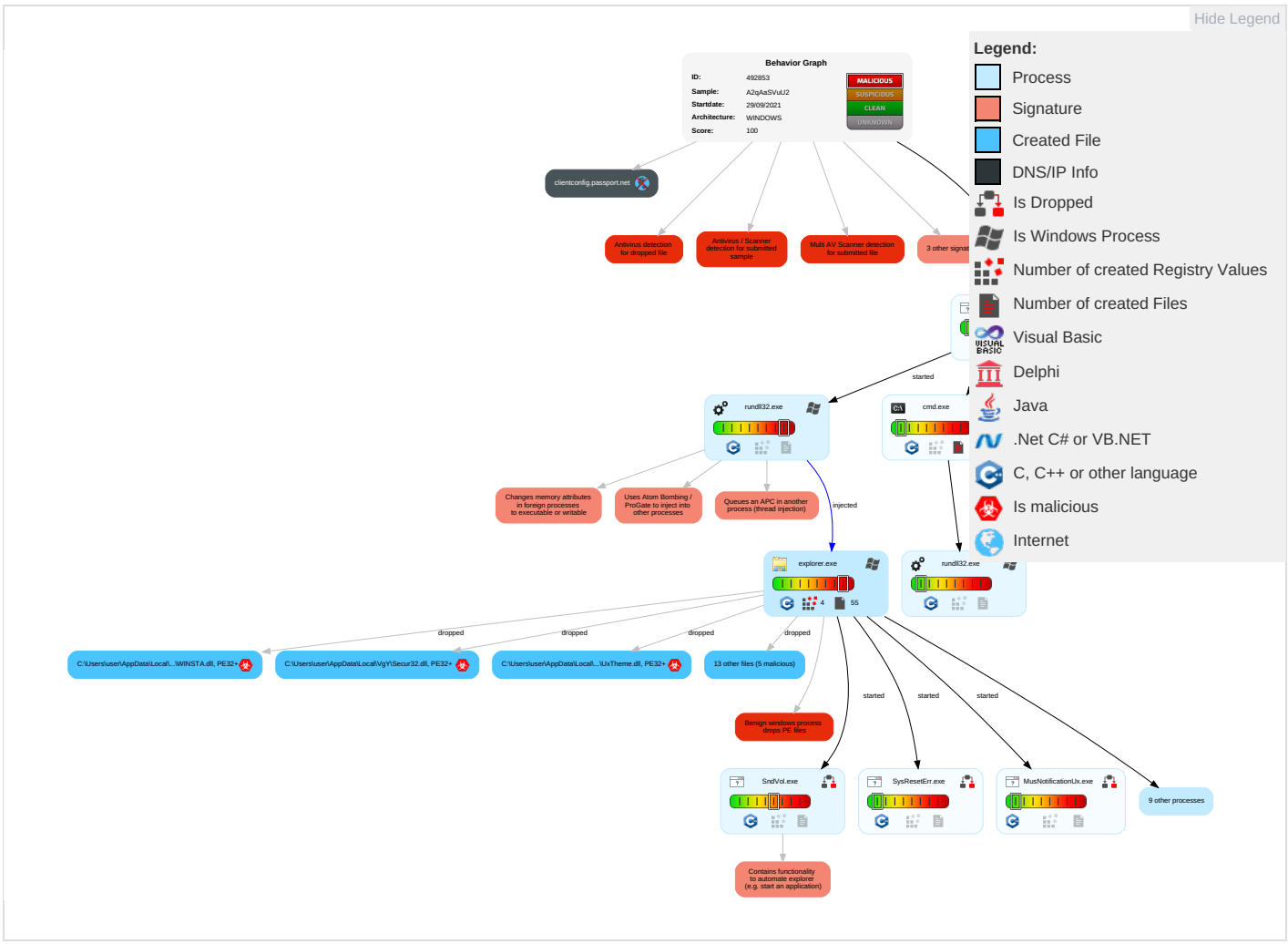
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping	System Time Discovery 1 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2
Default Accounts	Exploitation for Client Execution 1	Application Shimming 1	DLL Side-Loading 1	Obfuscated Files or Information 3	LSASS Memory	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Software Packing 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 1	Timestomp 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatior
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	DLL Side-Loading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

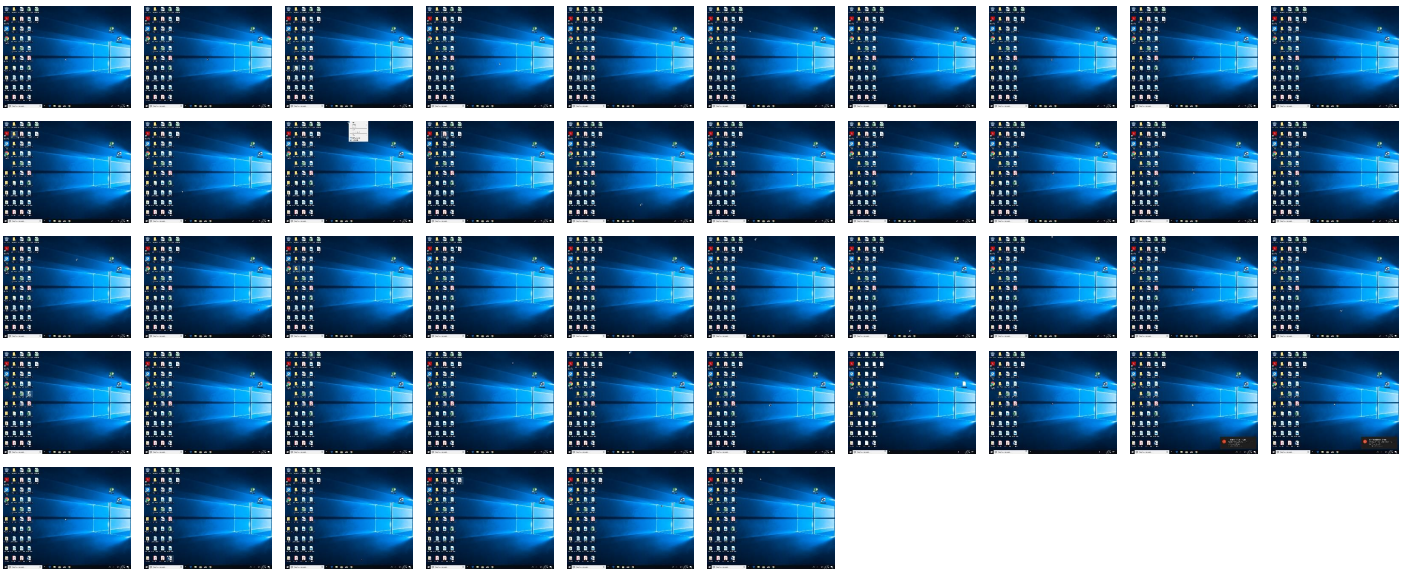
Behavior Graph



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
A2qAaSVuU2.dll	65%	Virustotal		Browse
A2qAaSVuU2.dll	63%	Metadefender		Browse
A2qAaSVuU2.dll	84%	ReversingLabs	Win64.Infostealer.Dridex	
A2qAaSVuU2.dll	100%	Avira	HEUR/AGEN.1114452	
A2qAaSVuU2.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\A1gpxNou\ReAgent.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\FQTqHJ\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\AxQmthi0\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\wsL8xMIEF\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\NNd0CnGJ\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\VgY\Secur32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\A1gpxNou\ReAgent.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\FQTqHJ\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\AxQmthi0\DUI70.dll	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\wsL8xMIEF\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\NNd0CnGJ\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\VgY\Secur32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\A1gpxNou\RecoveryDrive.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\A1gpxNou\RecoveryDrive.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.RecoveryDrive.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.EhStorAuthn.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.SysResetErr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.mstsc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.MusNotificationUx.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.SndVol.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.micro	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clientconfig.passport.net	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492853
Start date:	29.09.2021
Start time:	03:36:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	A2qAaSVuU2 (renamed file extension from none to dll)
Cookbook file name:	default.jbs

Copyright Joe Security LLC 2021

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:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@40/17@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.1% (good quality ratio 16.8%) • Quality average: 40.6% • Quality standard deviation: 40.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\A1gpxNou\ReAgent.dll

Process:	C:\Windows\explorer.exe

C:\Users\user\AppData\Local\A1gpxNou\ReAgent.dll	
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.4118132531393357
Encrypted:	false
SSDEEP:	12288:yVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:vfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	FC9474302D7FD9538FC834CE63E1FD5C
SHA1:	290D8D20C7815ABC8918D60E44A9BF9BE063FDE1
SHA-256:	D7F76A8DB8CD5CBD47B91536221521A44BF8DD57E72EDF8C9239EB32F6165CCB
SHA-512:	01EBF58C36BB74763D7AB3D62AF275F35719EF0CC2CDFD742D113714C12130D614F4FBC8EDABAF9962580DE13025FE08BAEF4C435BAD242F8C979318D13424 E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.; ..DN^....." .....p.....@..... "....@lx}..b....."....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\A1gpxNou\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
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\AxQmthi0\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2519040
Entropy (8bit):	3.9419943640965944
Encrypted:	false
SSDEEP:	12288:MVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1nlplj:5fP7fWsK5z9A+WGAW+V5SB6Ct4bnbzl
MD5:	298E377EADD0706C1D73ADDEB77B8178
SHA1:	525213210DE858C13235C917106BB95C540F79F0
SHA-256:	70104ECBFB1142438426E2A5A0A4D7F3A50F65205F546CCF887A148065DB3CD4
SHA-512:	94D8B5C907339C786BF6CB9E49EC64783EA9E4F69988DA2729AE9728DD756C80850FFC4D9B5DAC2F44890BCB486B2442524E0B7AFFC215BE44C5B3E061C6E0 5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.; ..DN^....." .....P".....p.....@.....p&.....@lx}..b....."..dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\AxQmthi0\SysResetErr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	42392
Entropy (8bit):	5.943178981884173
Encrypted:	false
SSDEEP:	768:zYVfzVTBuXwMHhrdXbsxoXF8Q0no8pV1Pxo:CfuXXrdrXXD0no8xPxo
MD5:	6A3F2F3C36FE45A87E3BFA80B6D92E07
SHA1:	8C211767AD8393F9F184FC926FE3B8913F414289
SHA-256:	069608FF0FF5918681A80CF7603275DC6CD7D416A73D033D19962B0F0F1E1EAC
SHA-512:	A75669E0481901FC7CFCA55FBC7BD7FC0E8636767537017A41B1C720F34B5AD45AC75555D0AD246AC0DF670FDC31CBA1BEFD21D63E112AD427472DE3EA59CA6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%7..aV..aV..aV..h.S.cV...2..cV...2..vV...2..kV...2..tV..aV...V...2..oV..2?.`V...2..`V..RichaV.....PE..d...v.+J....."....6...X.....9.....@.....l..... .....!.....,...0t..T.....`d..(...`c.....d..`.....text...{4.....6..... ..`.imrsiv.....P.....rdata.....`...0...:.....@..@.data...h.....j.....@....pdata.....n.....@..@.rsrc.....t.....@..@.reloc.,.....@..B.....

C:\Users\user\AppData\Local\FQTqHJ\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
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.....@....pdata...x.....@..@.didat..x.....@....rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\FQTqHJ\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.406611949592817
Encrypted:	false
SSDEEP:	12288:WVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:LfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	CB757D9BD0E289A106808C0230A026A6
SHA1:	1F11AE588A68B3A2A29668CBD5A0A8A445E4938F
SHA-256:	450A946EC012C1311B599992FD920623C478F9B69FE246296AD6F8E9B57D0581
SHA-512:	DBD27A1ACA3AF8A626D4A4C80B46D394C936B1BCBF500255CAB63E42B8E2194FC82B694DC0A230236271F41A3B89AD2E8C2B57277A9E83F6B96F388E9A27237B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.;..DN^....." .....p.....@..... "....@lx}..b.....".....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\NNd0CnGJ\Magnify.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

C:\Users\user\AppData\Local\NNd0CnGJ\Magnify.exe	
Category:	dropped
Size (bytes):	809472
Entropy (8bit):	6.649005640850081
Encrypted:	false
SSDEEP:	6144:g4yELxB+4i7juGW9ku9gi9m5SBo3BZHgnlWXL1ogREJwkz5gzNOx8XA08bAhMWUy:1tLvDNhg0Pnomt8XOykpyk
MD5:	F97BE20B3744572366666607EE4BA7F7F
SHA1:	378D5ADAB450032CBD086A419C07DF8278FF4F32
SHA-256:	72A31AEB7655343C7112085DFD49A2D5F1A6F1191D8F91A96BC446DE932724EA
SHA-512:	62C8875A9ECB710CCE5CACBEFF3615A9771913F0C7A7CD42FFFE1D00F9B9E26D01139501635F1578F1B63E03682B52312E776A7191F291B86960B1D7464AB216
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._T..>:D.>:D.>:D.F.D.>:D.Z>E.>:D.Z9E.>:D.Z?E.>:D.Z;E.>:D.>;D.8 :D.Z3E.>:D.Z.D.>:D.Z.D.>:D.Z8E.>:DRich.>:D.....PE..d...U.....". ....@..... `..... .....8.....0.. @G.....-.....8...P"..T..... ...(... .....H...(.....text...\*..... ..`.rdata..t(.....*.....@..@.data.....@....pdata...-.. .....@..@.rsrc...@G...0...H.....@..@.reloc..8.....T.....@..B..... .....

C:\Users\user\AppData\Local\NNd0CnGJ\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.408793605428252
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0CA5F4D66EBB41C5D3F7E5A6D341F77F
SHA1:	3894DC22432580634AD98F990355CF0C15F10DD8
SHA-256:	31FA6F8CCF9DD4024AF161774599C6196118660437B4149DCDE28026B7A2478E
SHA-512:	A59C7EE98E855637B31C030D66611402D1D5106593FC633C7FB0793AA9B9C74296CA41960F9EA4FCF23568D1682CE1A9602D40496610B84D882466FE861F1E9B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.; ..DN^....." .....p.....@..... "....@lx}..b....."....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\QiP6c\SndVol.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259904
Entropy (8bit):	5.955701055747905
Encrypted:	false
SSDEEP:	3072:UfYIZJbRydnidilSnGvLqeD358rwW39nuyHjVozZcxSHfcBL1ljbEyB7HbIa+:Uf9JonidFnqLV358rNnJqcRcy10/
MD5:	CDD7C7DF2D0859AC3F4088423D11BD08
SHA1:	128789A2EA904F684B5DF2384BA6EEF4EB60FB8E
SHA-256:	D98DB8339EB1B93A7345EECAC2B7290FA7156E3E12B7632D876BD0FD1F31EC66
SHA-512:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B498 4
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.BL]..L]..L]..E%...]..#9..O]..#9..U]..#9..F]..#9..W]..L]...\..#9..o].. #9k.M]..#9..M]..RichL].....PE..d...wJSn.....". .....@..... .....p.... ..@.....@+...0..... ..U..T.....p&..(...p%.....&.....P.....text..... ..`.imrsiv.....rdata..... .....@..@.data.....@.. ..pdata.....@..@.didat.....@....rsrc...@.... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.4158562242471984

C:\Users\user\AppData\Local\QiP6c\UxTheme.dll	
Encrypted:	false
SSDEEP:	12288:HVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ufP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	7F591E3E13727BC65D9343A0424DC251
SHA1:	FB577F41F44AC64FFCAA911A382786B19BAC6DD5
SHA-256:	9C68174FA05C42FD588281AD3ED149DF3673A2932849410AC2E902772752871F
SHA-512:	6AA7DAA2DE4612E820E87182CDF95E8FFFFB7ADA175478F3F66F70C3B4E7BBA7FF3ECC29F31CD5C42C4BB85ACF5DE68CDAF55D8B54EF143B0FCB801B38434B49
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.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.;..DN^....." .....p.....@..... "....@lx}..b....."....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\VgY\Secur32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.417374163758923
Encrypted:	false
SSDEEP:	12288:KVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:XfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	DB5938B2BCF055E28A918103006CBCAA
SHA1:	87EFF0B3AE617315DDE7EBA2261EA88B7AF02061
SHA-256:	45561012881BCEB066C2F5A47ACA5F80D6463D025DE36DC19F54DB2A6D0DC216
SHA-512:	C6D17E4D7EBC15C78981A22DAABC9190C35F69239BD3AB714ADBFE3D39961D82059562CFA68EBBE6F1C1A8432472C76BBA4486C20D384302194E96C16470FEC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.;..DN^....." .....p.....@..... "....@lx}..b....."....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\VgY\mstsc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3640832
Entropy (8bit):	5.884402821447862
Encrypted:	false
SSDEEP:	98304:q8yNOTNEpZxGb+ZPgN6tYDNBMe+8noqvEYw0n2WFfZT+xgsLOsMg:q8yNOTNEpZxk+ZIN6tYDNBMe+8noqvEB
MD5:	3FBB5CD8829E9533D0FF5819DB0444C0
SHA1:	A4A6E4E50421E57EA4745BA44568B107A9369447
SHA-256:	043870DBAB955C1851E1710D941495357383A08F3F30DD3E3A1945583A85E0CA
SHA-512:	349459CCF4DDFB0B05B066869C99088BA3012930D5BBC3ED1C9E4CF6400687B1EFE698C5B1734BF6FF299F6C65DD7A71A2709D3773E9E96F6FDE659F5D883F4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... w.dN$.dN$.dN$..M%.dN$..J%.dN$..K%.dN$..O%.dN$.dOTfN..G%.eN$...$.dN$..L%.dN$Rich.dN$.....PE..d.....Y.....".....$....%.....p.....@.....7.....K8...`.....].....p..H>!.....`.....7. *..P...T.....`.....`.....\..`.....text....".....$..... ..`.rdata...\...@..^...(.....@..@.data...P(.....@....pdata..`.....@..@.didat..(....`..... .....@....rsrc...H>!..p...@!..".....@..@.reloc.. *....7.,...b7.....@..B.....

C:\Users\user\AppData\Local\r1aQ\EhStorAuthn.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	128512

C:\Users\user\AppData\Local\r1aQ\EhStorAuthn.exe	
Entropy (8bit):	6.2177431661699805
Encrypted:	false
SSDEEP:	1536:JkvDU6Ogd6+nGNj73upR/yc4jKxyB6zd23W9aMEbq6GIwc0eomgPHA5kG9mQ7N6A:bgd6+E3ueD+bc0xPxQZDFcZIZ
MD5:	5B9BB7B6DD9A81D42F057BA252DC3B63
SHA1:	EC0699019DF4B9BC7D12C4B3CAFC4963210B5C7A
SHA-256:	4348A9C263028C665AA486B08DDD22BC7F3879B0A89765DA5A0F4AECD0A1224C
SHA-512:	9F77B1720CB1F3218556E396B264A15765FF8925FFFBEF1121245BB7F15174EBC7A2C341AD787410F326EE2E18EC097DE191F21B8B4335C1129EB41289E68E19
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)S..H=@.H=@.H=@.,>A.H=@.,9A.H=@.,8A.H=@.,<A.H=@.H<@ "H=@.,4A.H=@.,=A.H=@.,.@.H=@.,?A.H=@Rich.H=@.....PE..d....G.....".....^.....`.....@.....0.....`..... .....`..`..... .....\..... .,.,.. ...T.....8.....text..... ..`.rdata..f.....0.....@..@.data.....@....pdata..\..... .....@..@.rsrc.....@..@.reloc..,.... .....@..B..... .....

C:\Users\user\AppData\Local\r1aQ\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2236416
Entropy (8bit):	3.4158800780354133
Encrypted:	false
SSDEEP:	12288:VVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:MfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4D29023178FD2D10CB3ACE4885820458
SHA1:	140E9C96A2D4A8BAC949B02FB928E0FF76754B6E
SHA-256:	FEA11ED22EBAA8A456516620C8B73281104BE7E328AD6FE82C9E013216E3EF7A
SHA-512:	0F935996AFF73EA5FBB0CE613229D31D4D0F2FD37C7207B4987D464E12A1FD2F14E45E5DEE001069144C45F35B9D0825CCF72AC46E8487A7FCA22879C3D555E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.; ..DN^....." .....p.....@..... "....@lx}..b.....".....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\wsL8xMIEF\DisplaySwitch.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1930224
Entropy (8bit):	1.9511202288226894
Encrypted:	false
SSDEEP:	3072:LvyYYIF4cmwcTigBmZWRHLxgMNnVYvkkVp66oB4E7p6:LvyYBF4R/igoZWRryMNnqz3
MD5:	97411B8A84E5980E509E500C3209E5C0
SHA1:	23398F8DA469DEAF10C32773062A6A62B7B004B4
SHA-256:	2C968556FCAD7EBB9A866B21A9F3F3DFCD0CA490CAF8F6B2ECDB423B9D24D3EF
SHA-512:	1D5E598B51B37E8A92FA188A8D59C67B7522480B46AFB5D2033D4380A3C5A120D0DB2BE6FE62B636A23AD83F757B7A1803B77A0EA19DF3C51B9BD36B0F06CB A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..zd..)d..)d..)m.T)R..)...(g..)...(q..)...(c..)...(E..)d..)...)...({..)..8)e..)... (e..)Richd..)........PE..d....[~....."..... ....@.....`..... .....\.....(3.....d.....c...P..X.....T.....K..(....J..... ....K..x.....text..... ..... ..`.imrsiv.....0.....rdata..6....@.....$.....@..@.data...(.....@....pdata..d..... .@..@.rsrc...(3.....4.....@..@.reloc..X....P.....@..B..... .....

C:\Users\user\AppData\Local\wsL8xMIEF\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2240512
Entropy (8bit):	3.4238232767891454
Encrypted:	false
SSDEEP:	12288:bVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:6fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	447058F8460FC604A0852CCD62462C97
SHA1:	E2B5CE7A28224F839FA0B4A153F6B01A8C70586E

C:\Users\user\AppData\Local\wsL8xMlEF\WINSTA.dll	
SHA-256:	B0BBEEB74A6BAE9B3AAB49327F807FEE63018C92342E4CBFA3B2666F2AFAB0F0
SHA-512:	BD751199866B6C07BAED02AA233E9A012845BAAA91659853C0F8A6E24749F37796A32E75AAF042498865E818BD9B6B25694D9A60D89ADEAE1ADE623A6FE6CC0 3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.; ..DN^....." .....p.....@.....0".....@lx}..b.....".m....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

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):	4447
Entropy (8bit):	5.479118735651339
Encrypted:	false
SSDEEP:	48:JpnURyDsHPcrkR/J6AhUzHrpnUnLpM/Fuc2/7h6OSJXJY8LU+QYwBMuMuEu:JJGymPcmJfhU3JadubugTXs+QYwKLu
MD5:	F4F1FA09A467998A8BCD1E6EA05488A7
SHA1:	CB33AC91E6108330488B353C5BBE786087F35AD3
SHA-256:	D639226D41D26952376E2C91BFD87D04BF284E895A4D9446FEE48F53F37519C9
SHA-512:	6FBDA3141C980C94E85C54DBBFB084204183F133D04DCE98525E80FF62E2A33E1C2D7D2133232871E8D7DB5CD51C8AE9A73EE469E18E741672DDA6C157EDBF 9
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....vf..G..~^D.....O@.....w..5..-.L....W.}.P.....K.....Hkk\.#Y...y... ..-_..C..j..3..i&.. t.#..5...d.....z..O.....6r...G..V..q.J....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....W...RX..}.<%...K.V.\._.y..F..... ...oB.....:..C@.....xM.6H.M.#.....:..Kk.- K.y.vK.....s.O.k..%2.....(gv.sNcW..c.....t.nc..''S...L)....2.k.|3.....].p..y-(..h.C.a)Y....E.@p..g.?.-.zI.y.....ku..!1...o.kZ.bzZ.y.....K/.K.Yn.O.... ..Z.....i.8.>.....^.5K...]#...6|.... .3.NW..7.R@(/e.u;.N...~[..i..K.H....}...V!`....A.).7.....-.....4E<.f.8.^.ZQU..xj...\..w...3k_..TmE8$.....m.....3I.U..%..1.].H.@.YM.....'.....(.?..{....X..&.....hzk`...../p+.....;. ..b....w'P..5Om>.._...f.{...l...T.....5a@T.1.iW{.N.hlV5.... :O.T_$.l..&\..Mz.z..{.f...F7..N..F*.c....*h.O

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.4112191453962337
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:	A2qAaSVuU2.dll
File size:	2232320
MD5:	f8295446e335b679641637334c99242d
SHA1:	18b9a40791f1a52c70507b29d0b631510f2e33c6
SHA256:	96705595655fd817156073e3d3efde3338e24c3afaef13e517153ae4b5218fc9
SHA512:	82b140666adcf81d786ef650a4eeae44a133c23593e2ccb14a1bd0b262084dd937d2fe6546fd691ba859b376becbfc4f18e57459d8e9e6b2e20654cc227fd1b7
SSDEEP:	12288:/VI0W/TtlPLfJCm3WlYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:2fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
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:	0x5E4E44CC [Thu Feb 20 08:35:24 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:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64fd0	0x65000	False	0.702641553218	data	7.86628806834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x880	0x1000	False	0.139892578125	data	1.23838501563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0x2324	0x3000	False	0.0498046875	data	4.65321444248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.qkm	0xc4000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvjb	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlmkv	0xc7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wucsxe	0xc8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fltwtj	0x10e000	0x1267	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sfplio	0x110000	0x736	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
.rpg	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bewzc	0x157000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vksvaw	0x159000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wmhg	0x15a000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kswemc	0x15c000	0x36d	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kaxfk	0x15d000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wualk	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qdxz	0x160000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rkyg	0x161000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.psul	0x162000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pyjm	0x163000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eoadme	0x164000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fnz	0x165000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gwheg	0x166000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fcd	0x1ac000	0x322	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dwk	0x1ad000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hgy	0x1ae000	0xae7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nfm	0x1af000	0x46e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qmfqd	0x1b0000	0xd57	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.buzyfh	0x1b1000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.towo	0x1b2000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.omwdbg	0x1b3000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.virw	0x1b4000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bck	0x1bb000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mbhfb	0x1bc000	0x573	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kix	0x1bd000	0x896	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
.gurzs	0x1be000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dzdoj	0x1bf000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.egret	0x1c0000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ftpyc	0x1c2000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qrc	0x1c3000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tnnx	0x1c4000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vsjhk	0x1c5000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fmswwe	0x1c6000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zfhn	0x1c7000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ejdgrp	0x1ce000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.soyat	0x1cf000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jlil	0x1d0000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bojgf	0x1d1000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gvsnik	0x1d2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lsc	0x1d3000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uepvem	0x219000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.don	0x21a000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dqju	0x21c000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qmgrql	0x21e000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cjrd	0x21f000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Language of compilation system	Country where language is spoken	Map

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 03:38:58.077536106 CEST	192.168.2.5	8.8.8.8	0x6cdd	Standard query (0)	clientconfig.passport.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 03:38:32.352840900 CEST	8.8.8.8	192.168.2.5	0x2b7e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 03:38:48.043163061 CEST	8.8.8.8	192.168.2.5	0x9b72	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 03:38:58.108865976 CEST	8.8.8.8	192.168.2.5	0x6cdd	No error (0)	clientconfig.passport.net	authgfx.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 3104 Parent PID: 2456

General

Start time:	03:37:40
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe

Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll'
Imagebase:	0x7ff6977c0000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
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: 00000000.00000002.279916623.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5772 Parent PID: 3104

General

Start time:	03:37:40
Start date:	29/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll',#1
Imagebase:	0x7ff7eef80000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 2588 Parent PID: 3104

General

Start time:	03:37:41
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxFreeMemory
Imagebase:	0x7ff70a260000
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: 00000002.00000002.339300443.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3332 Parent PID: 5772

General

Start time:	03:37:41
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\A2qAaSVuU2.dll',#1
Imagebase:	0x7ff70a260000
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: 00000003.00000002.257940331.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 2588

General

Start time:	03:37:43
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 2436 Parent PID: 3104

General

Start time:	03:37:44
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxNewJob
Imagebase:	0x7ff70a260000
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: 00000006.00000002.263722595.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 800 Parent PID: 3104

General

Start time:	03:37:48
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A2qAaSVuU2.dll,DpxNewJobEx
Imagebase:	0x7ff70a260000
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: 00000007.00000002.274418377.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: SysResetErr.exe PID: 2876 Parent PID: 3472

General

Start time:	03:38:23
Start date:	29/09/2021
Path:	C:\Windows\System32\SysResetErr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SysResetErr.exe
Imagebase:	0x7ff650120000
File size:	42392 bytes
MD5 hash:	6A3F2F3C36FE45A87E3BFA80B6D92E07
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Reputation:	moderate

Analysis Process: SysResetErr.exe PID: 484 Parent PID: 3472

General

Start time:	03:38:32
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\AxQmthi0\SysResetErr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\AxQmthi0\SysResetErr.exe
Imagebase:	0x7ff727f80000
File size:	42392 bytes
MD5 hash:	6A3F2F3C36FE45A87E3BFA80B6D92E07
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: 00000015.00000002.387213363.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: RecoveryDrive.exe PID: 5932 Parent PID: 3472

General

Start time:	03:38:44
Start date:	29/09/2021
Path:	C:\Windows\System32\RecoveryDrive.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RecoveryDrive.exe
Imagebase:	0x7ff6a8220000
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: 6092 Parent PID: 3472

General

Start time:	03:38:45
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\A1gpxNou\RecoveryDrive.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\A1gpxNou\RecoveryDrive.exe
Imagebase:	0x7ff7bc7d0000
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: 00000018.00000002.415547508.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Copyright Joe Security LLC 2021

Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: MusNotificationUx.exe PID: 4756 Parent PID: 3472

General

Start time:	03:38:58
Start date:	29/09/2021
Path:	C:\Windows\System32\MusNotificationUx.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\MusNotificationUx.exe
Imagebase:	0x7ff6f7fe0000
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: 3940 Parent PID: 3472

General

Start time:	03:38:58
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\FQTqHJ\MusNotificationUx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\FQTqHJ\MusNotificationUx.exe
Imagebase:	0x7ff618af0000
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: 0000001D.00000002.442655730.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: SndVol.exe PID: 3532 Parent PID: 3472

General

Start time:	03:39:10
Start date:	29/09/2021
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	0x7ff759370000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08

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

Analysis Process: SndVol.exe PID: 1208 Parent PID: 3472

General

Start time:	03:39:12
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\QiP6c\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\QiP6c\SndVol.exe
Imagebase:	0x7ff74a7a0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
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: 00000022.00000002.470825407.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: EhStorAuthn.exe PID: 3016 Parent PID: 3472

General

Start time:	03:39:24
Start date:	29/09/2021
Path:	C:\Windows\System32\EhStorAuthn.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\EhStorAuthn.exe
Imagebase:	0x7ff786bf0000
File size:	128512 bytes
MD5 hash:	5B9BB7B6DD9A81D42F057BA252DC3B63
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: EhStorAuthn.exe PID: 2424 Parent PID: 3472

General

Start time:	03:39:26
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\r1aQ\EhStorAuthn.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\r1aQ\EhStorAuthn.exe
Imagebase:	0x7ff6f2320000
File size:	128512 bytes
MD5 hash:	5B9BB7B6DD9A81D42F057BA252DC3B63
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000024.00000002.501617051.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: mstsc.exe PID: 5972 Parent PID: 3472

General

Start time:	03:39:38
Start date:	29/09/2021
Path:	C:\Windows\System32\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mstsc.exe
Imagebase:	0x7ff7ab200000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mstsc.exe PID: 5668 Parent PID: 3472

General

Start time:	03:39:39
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\VgY\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\VgY\mstsc.exe
Imagebase:	0x7ff657d30000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
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: 00000029.00000002.529730818.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021