ID: 492878
Sample Name: yPeVDkBY3n
Cookbook: default.jbs
Time: 04:14:54
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report yPeVDkBY3n 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
E-Banking Fraud: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Rich Headers 17
Data Directories 17
Sections 17
Resources 18
Imports 18
Exports 18
Version Infos 18
Possible Origin 19
Network Behavior 19
Network Port Distribution 19
UDP Packets 19
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: loaddll64.exe PID: 6392 Parent PID: 496 19
General 19
File Activities 19
Analysis Process: cmd.exe PID: 6432 Parent PID: 6392 20
General 20
File Activities 20
Analysis Process: rundll32.exe PID: 6480 Parent PID: 6432 20
General 20
File Activities 20
File Read 20
Analysis Process: rundll32.exe PID: 6488 Parent PID: 6392 20
General 20
File Activities 21
File Read 21

Analysis Process: explorer.exe PID: 3292 Parent PID: 6480 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Registry Activities 21
Key Created 21
Key Value Created 21
Analysis Process: rundll32.exe PID: 6552 Parent PID: 6392 21
General 21
File Activities 22
File Read 22
Analysis Process: rundll32.exe PID: 6728 Parent PID: 6392 22
General 22
File Activities 22
File Read 22
Analysis Process: Netplwiz.exe PID: 2848 Parent PID: 3292 22
General 22
Analysis Process: Netplwiz.exe PID: 3584 Parent PID: 3292 22
General 22
File Activities 23
File Read 23
Analysis Process: recdisc.exe PID: 6784 Parent PID: 3292 23
General 23
Analysis Process: recdisc.exe PID: 6696 Parent PID: 3292 23
General 23
File Activities 23
File Read 23
Analysis Process: phoneactivate.exe PID: 6768 Parent PID: 3292 23
General 23
Analysis Process: phoneactivate.exe PID: 4116 Parent PID: 3292 24
General 24
File Activities 24
File Read 24
Analysis Process: wermgr.exe PID: 5968 Parent PID: 3292 24
General 24
Analysis Process: wermgr.exe PID: 6056 Parent PID: 3292 24
General 24
File Activities 25
File Read 25
Analysis Process: wermgr.exe PID: 4068 Parent PID: 3292 25
General 25
Analysis Process: wermgr.exe PID: 7096 Parent PID: 3292 25
General 25
Analysis Process: rdpinput.exe PID: 4312 Parent PID: 3292 25
General 25
Analysis Process: rdpinput.exe PID: 5240 Parent PID: 3292 26
General 26
Disassembly 26
Code Analysis 26

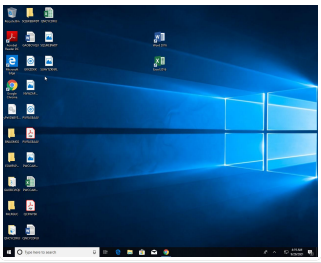
Windows Analysis Report yPeVDkBY3n

Overview

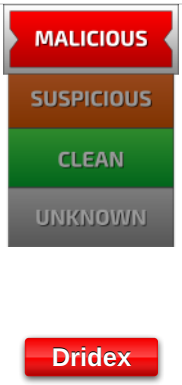
General Information

Sample Name:	yPeVDkBY3n (renamed file extension from none to dll)
Analysis ID:	492878
MD5:	2cd9944b4c5163..
SHA1:	fbbe87d4587c694.
SHA256:	a92176c5e1216a..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

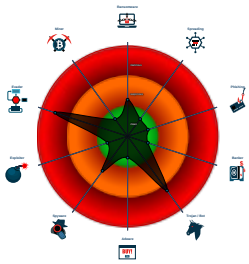


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Queues an APC in another process …
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Queries the installation date of Wind…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6392 cmdline: loaddll64.exe 'C:\Users\user\Desktop\yPeVDkBY3n.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 6432 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\yPeVDkBY3n.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6480 cmdline: rundll32.exe 'C:\Users\user\Desktop\yPeVDkBY3n.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - Netplwiz.exe (PID: 2848 cmdline: C:\Windows\system32\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
        - Netplwiz.exe (PID: 3584 cmdline: C:\Users\user\AppData\Local\SbH2\Netplwiz.exe MD5: A513A767CC9CC3E694D8C9D53B90B73E)
        - recdisc.exe (PID: 6784 cmdline: C:\Windows\system32\recdisc.exe MD5: D2AEFB37C329E455DC2C17D3AA049666)
        - recdisc.exe (PID: 6696 cmdline: C:\Users\user\AppData\Local\r4gbgdji\recdisc.exe MD5: D2AEFB37C329E455DC2C17D3AA049666)
        - phoneactivate.exe (PID: 6768 cmdline: C:\Windows\system32\phoneactivate.exe MD5: 09D1974A03068D4311F1CE94B765E817)
        - phoneactivate.exe (PID: 4116 cmdline: C:\Users\user\AppData\Local\lW7exk8\phoneactivate.exe MD5: 09D1974A03068D4311F1CE94B765E817)
        - wermgr.exe (PID: 5968 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
        - wermgr.exe (PID: 6056 cmdline: C:\Users\user\AppData\Local\JaJWNKcB\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
        - wermgr.exe (PID: 4068 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
        - wermgr.exe (PID: 7096 cmdline: C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
        - rdpinput.exe (PID: 4312 cmdline: C:\Windows\system32\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
        - rdpinput.exe (PID: 5240 cmdline: C:\Users\user\AppData\Local\iBq\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
  - rundll32.exe (PID: 6488 cmdline: rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6552 cmdline: rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6728 cmdline: rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.362816566.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.334340057.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.458324438.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001B.00000002.388799941.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000A.00000002.267627821.0000000140001000.00000020.00020000.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

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)

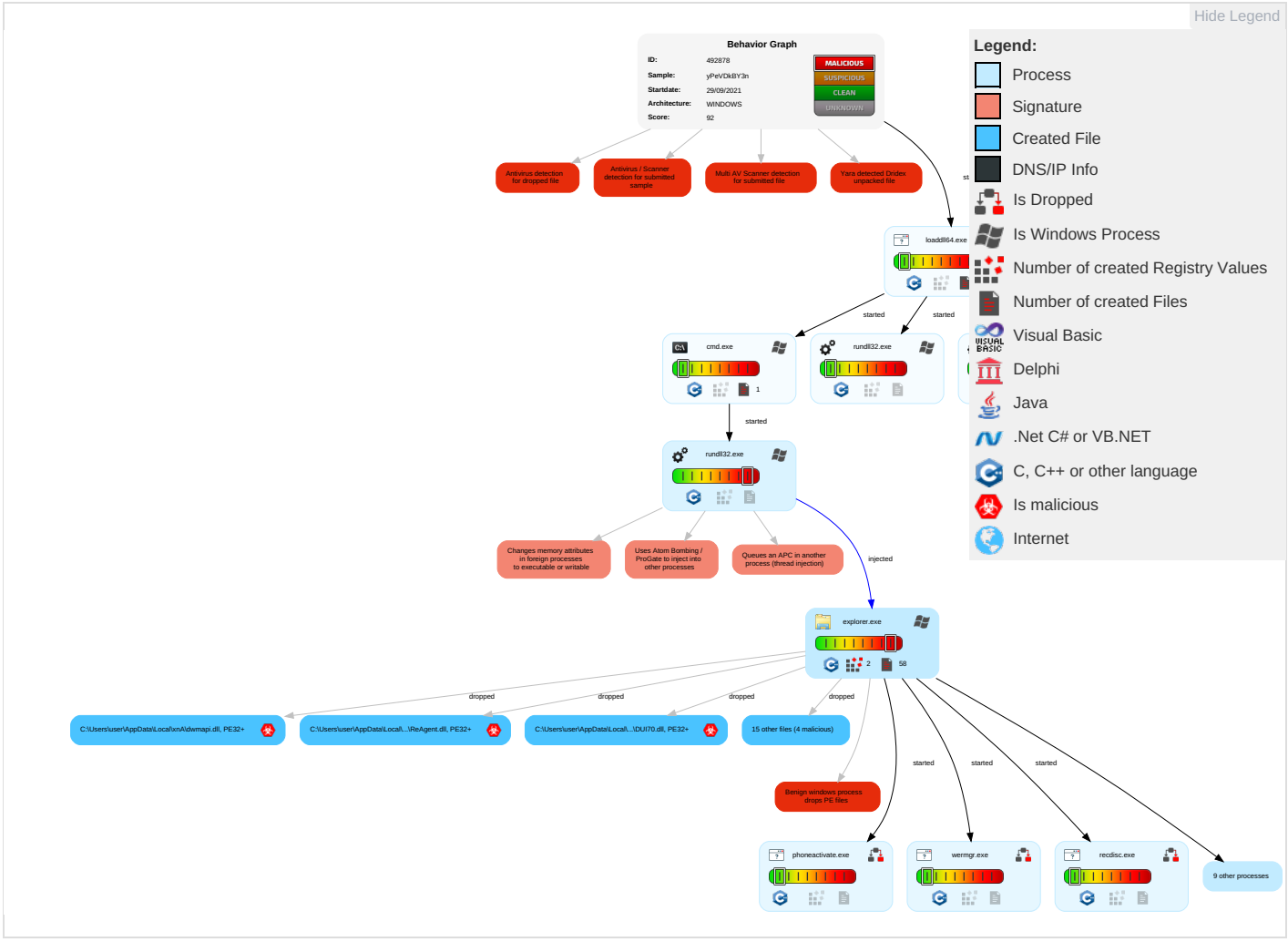
Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Service Execution 2	Windows Service 2	Windows Service 2	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Exploitation for Client Execution 1	Application Shimming 1	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Process Injection 3 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Information Discovery 3 6	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

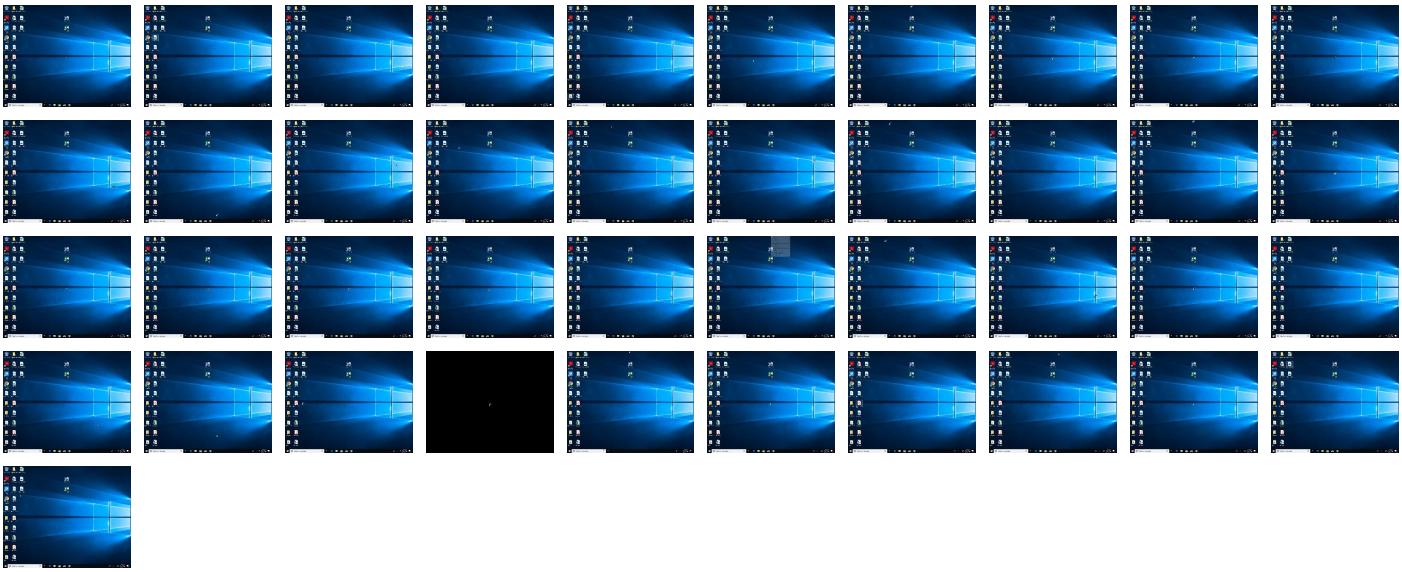
Behavior Graph



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
yPeVDkBY3n.dll	64%	Virustotal		Browse
yPeVDkBY3n.dll	63%	Metadefender		Browse
yPeVDkBY3n.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
yPeVDkBY3n.dll	100%	Avira	HEUR/AGEN.1114452	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\iBq\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\xnA\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\SbH2\NETPLWIZ.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\02vERQ6Eo\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\NMBpLf1V\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\r4gbgdji\ReAgent.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\02vERQ6Eo\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\lW7exk8\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\02vERQ6Eo\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.rdpinput.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.wermgr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.phoneactivate.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.wermgr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.recdisc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.Netplwiz.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492878
Start date:	29.09.2021
Start time:	04:14:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yPeVDkBY3n (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.evad.winDLL@41/19@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.6% (good quality ratio 38.1%) • Quality average: 46.8% • Quality standard deviation: 41.3%
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe	td1i2JJWLZ.dll	Get hash	malicious	Browse	
	TDhTkVMvVd.dll	Get hash	malicious	Browse	
	ShmrlNrhab.dll	Get hash	malicious	Browse	
	knYgnOrOXk.dll	Get hash	malicious	Browse	
	Dk62bv8zDb.dll	Get hash	malicious	Browse	
	UVkobIdWdL.dll	Get hash	malicious	Browse	
	EeshGc2wcs.dll	Get hash	malicious	Browse	
	3XSR1oCsva.dll	Get hash	malicious	Browse	
	9kiaVokmF5.dll	Get hash	malicious	Browse	
	90eZiqkJTL.dll	Get hash	malicious	Browse	
	e75OHzYF9S.dll	Get hash	malicious	Browse	
	BddeqTej4A.dll	Get hash	malicious	Browse	
	DC2zX44MQr.dll	Get hash	malicious	Browse	
	AUThpzgw53.dll	Get hash	malicious	Browse	
	Yz2OIFLI6N.dll	Get hash	malicious	Browse	
	RpwMYPzTGV.dll	Get hash	malicious	Browse	
	62sLZtD8d8.dll	Get hash	malicious	Browse	
	X5C9EzCB7A.dll	Get hash	malicious	Browse	
	aaPdM4E7Kv.dll	Get hash	malicious	Browse	
	bHcIZ7Xm3U.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\02vERQ6Eo\wer.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2338816
Entropy (8bit):	3.29446783991526
Encrypted:	false
SSDEEP:	12288:FVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:cfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1473BA39831B2BB5DA9797CF8A760752
SHA1:	ABCA22697FCAAD2585A730FB64A90222A08E751B
SHA-256:	13B0EC43B346CE31DB4034996B76E6605A3DBE8BDEB5171F148AF838532F3427
SHA-512:	0DE8E20350A369622B204B5427F58219DF6F0D98107A8CBCEE8362FB5DF7049DCC791D85B82B66D29C63275D462EE46C0F44B5E5D74FECBC66193C245881429
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d. ..DN^....." .....p.....@.....#.....@lx}..b.....#.W....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe

Process:	C:\Windows\explorer.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:	24073F60B886C58F227769B2DD7D1439DF841784E43E753265DA761801FDA58FBEEDAC4A642E0A6ABDA40A6263153FAA1A9540DF6D35E38BF0EE5327EA55B4FE
Malicious:	false

C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe	
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: td1i2JJWLZ.dll, Detection: malicious, Browse • Filename: TDhTkVMvVd.dll, Detection: malicious, Browse • Filename: ShmrlNrhab.dll, Detection: malicious, Browse • Filename: knYgnOrOXk.dll, Detection: malicious, Browse • Filename: Dk62bv8zDb.dll, Detection: malicious, Browse • Filename: UVkobIdWdL.dll, Detection: malicious, Browse • Filename: EeshGc2wcs.dll, Detection: malicious, Browse • Filename: 3XSR1oCsva.dll, Detection: malicious, Browse • Filename: 9kiaVokmF5.dll, Detection: malicious, Browse • Filename: 90eZiqkJTL.dll, Detection: malicious, Browse • Filename: e75OHzYF9S.dll, Detection: malicious, Browse • Filename: BddeqTej4A.dll, Detection: malicious, Browse • Filename: DC2zX44MQr.dll, Detection: malicious, Browse • Filename: AUThpzgw53.dll, Detection: malicious, Browse • Filename: Yz2OIFLI6N.dll, Detection: malicious, Browse • Filename: RpwMYPzTGV.dll, Detection: malicious, Browse • Filename: 62sLZtD8d8.dll, Detection: malicious, Browse • Filename: X5C9EzCB7A.dll, Detection: malicious, Browse • Filename: aaPdM4E7Kv.dll, Detection: malicious, Browse • Filename: bHcIZ7Xm3U.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.jl..jl..jl..c1...l...-..il...-..ql..jl...H...-..ml...-..`l...-..Kl...-..kl...-..kl..Rich jl.....PE..d...p....."....,.....`(.....@.....p.....`..... .... ..0:.....!...`..\...@...T.....`Q.....`R.. ...t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@. .@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\....`.....@..B..... .....

C:\Users\user\AppData\Local\4S1sd\wbengine.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1535488
Entropy (8bit):	6.5079506357027785
Encrypted:	false
SSDEEP:	24576:UgSNpxTPrVDqUtzohGP5ilEI1T4N9sS4aC+369riDQMbbKoLtHWwtPJhVx8OIC9h:UtNpxTPrVuUtMhGRuEAc3sfaYhiDXmod
MD5:	6E235F75DF84C387388D23D697D6540B
SHA1:	A97DE324726F3ECBA383863CB643E4AD5DADB4DC
SHA-256:	7113DD02243E9368EF3265CF5A7F991F9B4D69CAB70B1A446062F8DD714AFC8E
SHA-512:	F294A7F7AD6FAD1E2F2E82123AFB78B76E56C603EF3FA37CDD73992DE91640EB55E2F002072DD57B850B1D7E9162F49B4DE973CFE71DF35DAD958B439E1F287A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|r..|r..|r..q..|r..v..|r..w..|r..s..|r..|s..}r..{.M|r..r..|r.....|r..p..|r.Rich.|r..... .....PE..d...!.....".....z.....p.....@.....v....`..... .....|..... ...u.....@...T.....=..(....<..... (=.....text..... ..`.rdata..b.... .....@..@.data....&.....@....pdata...u... ...v.....@..@.rsrc.....Z.....@. .@.reloc.....f.....@..B..... .....

C:\Users\user\AppData\Local\4S1sd\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2338816
Entropy (8bit):	3.2944858495711675
Encrypted:	false
SSDEEP:	12288:WVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:LfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	3543EC05CA756B1F06EB2B0AACC9D942
SHA1:	4A9BDFA30309113CE909403BA861FE7DA61DBEA6
SHA-256:	5AFFA69FE77443A45448F840449A83A99ED5DC7305B9EDAD1B18E83920D6651A
SHA-512:	D5811F403386C4CF2A0BC9FCD2840E60C6E9D3728759D8F17DE29098F59E40B8479EBBB0A13ADF9F1996007E413A0ADF017BE869DE419B6DA34A0B7946F97A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d. ..DN^....." .....p.....@.....#.....@lx}..b.....#.W....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\JaJWNKcB\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\JaJWNKcB\wer.dll	
Size (bytes):	2338816
Entropy (8bit):	3.29446537113494
Encrypted:	false
SSDEEP:	12288:EVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ17:hfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	747B98D135003541875FAF52AC306E8C
SHA1:	48B2F6D5E0DD975C2317B57001CF76FA7E216FDB
SHA-256:	0E0A32F47BC17DCE5065B354B9D2D80F197171AAA21851C662ED5FAF4E06E2F9
SHA-512:	2EFFDF7DA31856CAC3D244EAB4D3D1B5A9BD75986F742EDD4F7C20C3F4090157D57D8EF623CFB38A89A4110068FA730F2B814D10AF456640E6C464C67E1F7E 4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d. ..DN^......" .....p.....@.....#.....@lx}..b.....#.W....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\JaJWNKcB\wermgr.exe	
Process:	C:\Windows\explorer.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:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.Jl..jl..jl..c1...l...-..il...-..ql..jl...H...-..ml...-..`l...-..Kl...-..kl...-..kl..Rich jl.....PE..d...p.....".....,.....`(.....@.....p.....`..... ... ..0:.....!...`..\...@...T.....`Q.....`R.. ...t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@. .@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\....`.....@..B..... .....

C:\Users\user\AppData\Local\NMBpLf1V\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2334720
Entropy (8bit):	3.2847498805521744
Encrypted:	false
SSDEEP:	12288:tVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:0fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	CC8967264AC0051358BBFA68E6427F00
SHA1:	D8730FCDE9EA727896962968C916B2CC7F2BEA4F
SHA-256:	CBFCA948E3B05DE0FD6379BCFBBA681BD92AAE312475273B676B79273480D566
SHA-512:	BF886CF6E5D769915D5DEF3EA7EEC60C52E2E892B2141003DFEFE443BC6E99B7E43C1E86517357CCB5F4763321D440EE17B26EDEA7FACC3198259637CCF765 2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
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\NMBpLf1V\SystemPropertiesProtection.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.065737112404973
Encrypted:	false
SSDEEP:	1536:YKuZAtREC/rMcgEPJV+G57ThjEC0kzJP+V5J8:+AzECTMpuDhjRVJGq
MD5:	B6C7834B60F72194E32822CD7F39D7A9

C:\Users\user\AppData\Local\NMBpLf1V\SystemPropertiesProtection.exe	
SHA1:	26AC4990B1203DD53A299857477EB2DE5CDC0DB1
SHA-256:	02F96A1E1233655997498DF6B11A48270DF05BDA561F004EDC83A165216A04C9
SHA-512:	96E8E380902866247A2873348C88DB244E87E1F925FF78AF06CE5541C5A1AA535BDA6DEB8941D646A1E7E91801BE934D715C990C96B5764511438BBE597D5F8A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d...k....."....."....>.....@.....{4....`..... .....&.....P..@'...@..... ...."..T..... .....!..8.....text..... ..`.rdata..N.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...@'...P...(..... .....@..@.reloc.. .....F.....@..B..... .....

C:\Users\user\AppData\Local\SbH2\NETPLWIZ.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2334720
Entropy (8bit):	3.28413644771884
Encrypted:	false
SSDEEP:	12288:nVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:OfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	5D08B0BB75667703159CEB7006226811
SHA1:	9A80743073CD75512FE4A9CD568B3F3AC71F519B
SHA-256:	BDF603FE8005AEF48DD0FE2A3A5924E23D14BAF77C908BE436511E595EFBD564
SHA-512:	357CA06848E9093FAE5C33498DDCA73829B19FF1AE8647D36CF0F647573372E791CDFBE196E2F7D67B4F14394AEFF603E64DE8687D6B207DC94B54EC9CDD3D5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
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\SbH2\Netplwiz.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.640119387300135
Encrypted:	false
SSDEEP:	768:Sm6uxIL0DPeyQvEsNN6hU2hGGalaQkQcryUJU3fUrh6WeENiJDBPrxZt4W:p6MMD6hlBBjrywUKeWSDBPrxZaW
MD5:	A513A767CC9CC3E694D8C9D53B90B73E
SHA1:	F10B719117D26DAFCC9DBE54E9F9D78A0F80EE2A
SHA-256:	C9F7AC4322504D7EC8305973951A66FBE34E55E34A59409B5B574D627A474369
SHA-512:	03BBBC076D3497E35952143085B9DCC83EDE855A00A190F05712FC91F0C0C4301995D0123EBDCA75A59B93C51358EAD5C4030F8EE9C33F9D1BF1A0EDBC52FD4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.K.U.K.U.K.U.B..G.U.$.P.J.U.$.V.H.U.$.Q.Y.U.$.T.F.U.K.T...U .$.\.J.U.$...J.U.$.W.J.U.RichK.U.....PE..d...v....."....n.....@6.....@.....`..... .....L.....F...p..... .....4....F..T.....@.....A.....text....-..... ..`.rdata..t....@.....2.....@..@.data.....`.....J.....@....pdata.....p..... ..L.....@..@.rsrc....F.....H...P.....@..@.reloc..4.....@..B..... .....

C:\Users\user\AppData\Local\iBq\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2338816
Entropy (8bit):	3.3011416970535334
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	94B821B5B1E458C1CB0B4A09B906F7B0
SHA1:	2A7FCEA73E2D92E83B845D89D8595BAE0FC676FB
SHA-256:	C264C3CF59F7D34D629B367B30BF57A0D9449C2448C9305FEAABB8CC7CAB1C23
SHA-512:	39FF14ED7990A54A1E535EF71B19BB77F36D4968A4279D1FF9CD67D63F649A7F194C62902BE8AA5479A1B2D18DFFE1079907E62AF9ADC95BE2DCDDAA423CB3DB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%

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

C:\Users\user\AppData\Local\iBq\rdpinput.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	178688
Entropy (8bit):	6.278002754824444
Encrypted:	false
SSDEEP:	3072:8i0hLL+KEukKO40+enSqroxn2JIQLtBDYiBJD3cR4DJSpzrA:10d/O40+8Sqk4ZLnBt2tp/
MD5:	4403785D297C55D5DF26176B4F1A52C8
SHA1:	4889F6E0B3CF649C3A8778779D7CEA534B9174B2
SHA-256:	7B8ED6EB50068D4C1B8E51F6F2E3604E6C3B6BB42C6D81ADD4C3B023B6386FF6
SHA-512:	3BAFC7BAE2586F05F05125BF34299D556D46F519D718DAEF8007A0B45D40B0D3CD794A4C55B93CBC1BA2DF111346E6012DEEAD0539AEA91BE71E8ABC877E51 1F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i..s:..s:..s:...s:..p;..s:..w;..s:..v;..s:..r;..s:..r:..s:..z;..s:...:..s:..q ;..s:Rich..s:.....PE..d...9`..... ".....  #.....@.....&m...`..... .....p.....d.....T.....A..... ....B.....text...s..... ..`.rdata..2n...0...p..."..... .....@..@.data.....@....pdata..d.....@..@.rsrc...p..... .@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\lW7exk8\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2617344
Entropy (8bit):	3.8188438649651406
Encrypted:	false
SSDEEP:	12288:ZVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1huj:YfP7fWsK5z9A+WGAW+V5SB6Ct4bnbhu
MD5:	62BE542D5399EB4FFA77F34146C89A06
SHA1:	C9C196CBF6C3E3ED6F4F75F4866FF368DBA3E733
SHA-256:	51A3092EC5597F8A2D20CFD605262809A24F5871C5D7DE3AC83C80D6EAF8FEEB
SHA-512:	675674438CA776ABAA99D4F3B89F255D7EA07D9202358661EB18B825661B260F0227982C0DA447EF941A73777266AD68D9484E80F8C4DCD3C469E9E9F8AC85C3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d. ..DN^....." .....#.....p.....@.....'.....@lx}..b.....#.dQ...c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\lW7exk8\phoneactivate.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107504
Entropy (8bit):	6.536585324272613
Encrypted:	false
SSDEEP:	1536:UhKYFAVrKO6PcIgpCaYov3ZKCZwaG70Ur/61cVtat/gLaoU0Sj09P0e:dmlPcNphvo0mtV1La8Lse
MD5:	09D1974A03068D4311F1CE94B765E817
SHA1:	7DD683571E4DCCAF181A5271BBCF15B3BC9D0155
SHA-256:	5D4F713CFC98E7148B67D063193D93BFE29F8329705A03690590633FADE32EE5
SHA-512:	07FD0700C8368485BEC91847C4B9721B059FEDB678C603A57FBD5DABCF110C80B0BD1D114384D4334F0412F3F4FD93C839A1B17F3A9F02C25CD59216692A8AC
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\IW7exk8\phoneactivate.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....O.....Rich..... ....PE..d.....^.....".....`.....@.....;;..... .....0.....p.. J...`.....~...%.....`"..T.....(..... .....text..... ..`.imrsiv.....rdata...I.....J.....@..@.data...8....P.....$.....@....pdata.....`.....&.....@..@.rsrc... J.. .p...L...0.....@..@.reloc.....|.....@..B..... .....

C:\Users\user\AppData\Local\r4gbgdji\ReAgent.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2334720
Entropy (8bit):	3.2894017306191445
Encrypted:	false
SSDEEP:	12288:fVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:WfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	BD93CFC880CD85449C09D257F59E7EB0
SHA1:	36145EE889672CEA943B718D0C7A56874AC47E2D
SHA-256:	443324951C2842D25EB7A9F8CDB562FCBF6A98AA744354C911E1467248F14AF9
SHA-512:	71DBD742B7D0C2A63F0C45663105E82224994FA8969D41A9C4732E631A2899F7E6358148DB7C00978FC6BB756951CB3B31339C49E17E6DB2D15F46342ECB5D8E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\r4gbgdji\recdisc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	6.154101271794163
Encrypted:	false
SSDEEP:	3072:H4SpDkUbgEHxW3BIovAuegPO8evTq2VC:H4/3BdFegEv+2V
MD5:	D2AEFB37C329E455DC2C17D3AA049666
SHA1:	69C5182FDC8A86009113EE721C8F1632F7B3D2DB
SHA-256:	A65F86E8EC62BEB3019E368E506DAB21FF872097EBF3FAEB4A3B23F2A08DFCE9
SHA-512:	DD5D63D79FD9E43560291687E0B41B71D6ECA55F033FE94BAA4FAF4CB967F6480CAC4F5481B3102F0589A65AFA473F5637B1C31C522329A275461F3D8C4353A3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e_...1...1...1..|....1..`5...1..`2...1..`4...1..`0...1...0...1..`8...1..`...1..`3 ...1.Rich..1.....PE..d...+38....."..... .....@.....@.....`..... .....|..... ..0.....0.....0m..T.....9.. (....8.....9.....text..... ..`.rdata...f...0...h.....@..@.data...`a.....Z.....@....pdata.....@..@.rsrc...0.... ... .@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\xnA\WMPDMC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1517568
Entropy (8bit):	6.62150533612437
Encrypted:	false
SSDEEP:	24576:esSffc55l2PlDph6LYq3BRf6Te8+n3wAJF1/Mk+F6uwY6V0qRr8kmHVJZh/u:cct2PpphUlxRn3wAblMk+F6+6S2r8/Hu
MD5:	4085FDA375E50214142BD740559F5835
SHA1:	22D548F1E0F4832AAEE3D983A156FDABD3021DA4
SHA-256:	93F61516B7FD3CE8F1E97F25B760BDF62AE58CC7714B559FEFC2C75AD1130804
SHA-512:	7712F8E551D475A9D2FF3BED9992A2B3D53AB01F61DCB7313320181F9EB6B5B84558CCA45AE95150267128C8B228F806F869157B7F4961755076DD83F02E3BDF
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....-.....*.....+...../...../.A.....'.X.....Rich..... .....PE..d...D..9....."..... .....@.....`..... ..... ..x.....l.....0...S..`Y..T.....G..(....F.....8G..... .....text..... ..`.rdata..Pg.....h.....@..@.data...p=...@.....,.....@....pdata..l.....D.....@..@.didat.....@.... rsrc...x.... .....@..@.reloc...S...0...T.....@..B..... .....

C:\Users\user\AppData\Local\xnA\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2334720
Entropy (8bit):	3.2895072698111227
Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	6D84A6C94112D7804EB1CC758C55B2CF
SHA1:	E6FFCE4E0BFDFA2C06617AE9580DB414C9E70920
SHA-256:	3832A03C486433934C446ADFD15C9FE87161C77716797CAE2DAB09B7A14A2EFA
SHA-512:	8700430F0F586309DAD71DF76E928887138D8D06E357E214929D979B416A23F20F71200DAF0347713649A54C41B6F012602229346FA8BEDD9C4C6976ACDEF709
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4462
Entropy (8bit):	5.481944559569596
Encrypted:	false
SSDEEP:	48:e+afUydu/etyBs1mM/p2h7Rl071riXrf8I+afUGdrZ4+GGx8u56DgCBnC5gCkHyf:edA/etNWcaj8IdhZ46Z6Xchkm3
MD5:	5BCBC228F6BDC12E0C1A9506C16268C0
SHA1:	E9A3B2AACA5DE93288F2715EEC42C0279833F97D
SHA-256:	D964D2C003C0D595492B8726ABEAA5F4C71DE847E4F263DAD1872FAD6FAF6DE6
SHA-512:	8254B7B248110E0A1F7EB69E3979BBA8B4CFA2AE07A79CB26DFF3D970693F4657281018EEBF45DED66A1BE8FA376F572E2E6C750BF03D38DD4E66721A396618F
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....4.....%d..S.|..Zl...69.3.L....o.....dh..f.Y.N.....A_....t..fS.p.:F.....3l)...a0...,F.Z3....Kk,X....S...M....q.....z..O.....a. ..NO..lP.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....|...T.....Q....<.G.v..... .....|.sl.\..c..g8.,....FW..S ..T.....u.;..... p&.:..h .)W.,. ..K..g.0....8.n..|.G.sg<MI....x).....{?....U...u.|Z^....k..3T.F...r..N...1..@.&....%cH.\B.},.4.d.....@.h...xC.....F..2Z.[}....j.'...+..T...[.+.%.A.5....X.Z...q.....vD@....aJ...4.....G.....*.r../|%....Bb..I-@..Y|<..''..(.....$C.x.J...S..^70J.$^$.&.8..!.b.!.....#.9..8D.qF...D.....4....8.JE.+K#U.|r..)..}..!..U%.fA.|.a..&...../.c.k..{..w*K...L.U5..G..o...T%7.+.]Q.A._c...=W.....&..!U.....b.X!.nsG..V..Q..eM.O4.g.T.] R.[.Q.....t|.../....w..N%1W..i.%!O..O.6q....[..z|.

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.199261302559909
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:	yPeVDkBY3n.dll
File size:	2330624
MD5:	2cd9944b4c51630053a486adf9ba7928
SHA1:	fbbe87d4587c694c6b44870bb99e30e1d48d1c06
SHA256:	a92176c5e1216a097c14b387a64e96684497919d0777250897db8896331613ca
SHA512:	3e532df504fe04dd632b9a719827a19e2353d216786013d0feb7b5f848cab6da07d565b7ee93e346f4c34c62a6ad7504a8c9f82d12303e2a205c297ff1e9bba

General

SSDEEP:	12288:i5VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1MVedA:i4fP7fWsK5z9A+WGAW+V5SB6Ct4bnbg
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	0x64f2c	0x65000	False	0.702390160891	data	7.86574512659	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.tblq	0x110000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hcmjm	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nagyk	0x157000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jrucz	0x158000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rnr	0x159000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ths	0x15a000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uuy	0x15b000	0x451c2	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.llcgmp	0x1a1000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zibji	0x1a2000	0xebe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nnbdme	0x1a3000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oxoht	0x1a4000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.poofxn	0x1a5000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yoxffm	0x1a6000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lbp	0x1a7000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cmyjh	0x1a8000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.khlpd	0x1a9000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ksydf	0x1ef000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jtgc	0x1f0000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ivi	0x1f2000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sqcys	0x1f3000	0x45174	0x46000	False	0.218484933036	data	5.76112633091	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	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6392 Parent PID: 496

General

Start time:	04:15:51
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\yPeVDkBY3n.dll'
Imagebase:	0x7ff64db90000
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: 00000001.00000002.273313020.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6432 Parent PID: 6392

General

Start time:	04:15:52
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\yPeVDkBY3n.dll',#1
Imagebase:	0x7ff7bf140000
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: 6480 Parent PID: 6432

General

Start time:	04:15:53
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\yPeVDkBY3n.dll',#1
Imagebase:	0x7ff63d4d0000
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: 00000004.00000002.334340057.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6488 Parent PID: 6392

General

Start time:	04:15:53
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff63d4d0000
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: 00000005.00000002.252235999.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6480

General

Start time:	04:15:54
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 6552 Parent PID: 6392

General

Start time:	04:15:56
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Imagebase:	0x7ff63d4d0000
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: 00000007.00000002.260064173.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6728 Parent PID: 6392

General

Start time:	04:16:00
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yPeVDkBY3n.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff63d4d0000
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: 0000000A.00000002.267627821.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: Netplwiz.exe PID: 2848 Parent PID: 3292

General

Start time:	04:16:34
Start date:	29/09/2021
Path:	C:\Windows\System32\Netplwiz.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Netplwiz.exe
Imagebase:	0x7ff69e8c0000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: Netplwiz.exe PID: 3584 Parent PID: 3292

General

Start time:	04:16:35
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\SbH2\Netplwiz.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\SbH2\Netplwiz.exe
Imagebase:	0x7ff7d7310000
File size:	39424 bytes
MD5 hash:	A513A767CC9CC3E694D8C9D53B90B73E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.362816566.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: recdisc.exe PID: 6784 Parent PID: 3292

General

Start time:	04:16:46
Start date:	29/09/2021
Path:	C:\Windows\System32\recdisc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\recdisc.exe
Imagebase:	0x7ff77db70000
File size:	192512 bytes
MD5 hash:	D2AEFB37C329E455DC2C17D3AA049666
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: recdisc.exe PID: 6696 Parent PID: 3292

General

Start time:	04:16:47
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\r4gbgdji\recdisc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\r4gbgdji\recdisc.exe
Imagebase:	0x7ff6c2000000
File size:	192512 bytes
MD5 hash:	D2AEFB37C329E455DC2C17D3AA049666
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: 0000001B.00000002.388799941.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: phoneactivate.exe PID: 6768 Parent PID: 3292

General

Start time:	04:17:00
Start date:	29/09/2021
Path:	C:\Windows\System32\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\phoneactivate.exe
Imagebase:	0x7ff724750000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: phoneactivate.exe PID: 4116 Parent PID: 3292

General

Start time:	04:17:05
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\lW7exk8\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\lW7exk8\phoneactivate.exe
Imagebase:	0x7ff6dc4c0000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
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.00000002.426654754.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: wermgr.exe PID: 5968 Parent PID: 3292

General

Start time:	04:17:18
Start date:	29/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff6db310000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: 6056 Parent PID: 3292

General

Start time:	04:17:20
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\JaJWNKcB\wermgr.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\JaJWNKcB\wermgr.exe
Imagebase:	0x7ff7e2150000
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: 00000024.00000002.458324438.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: wermgr.exe PID: 4068 Parent PID: 3292

General

Start time:	04:17:32
Start date:	29/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff6db310000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: 7096 Parent PID: 3292

General

Start time:	04:17:32
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\02vERQ6Eo\wermgr.exe
Imagebase:	0x7ff75f9b0000
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: 00000027.00000002.485059141.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: rdpinput.exe PID: 4312 Parent PID: 3292

General

Start time:	04:17:44

Start date:	29/09/2021
Path:	C:\Windows\System32\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rdpinput.exe
Imagebase:	0x7ff673710000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rdpinput.exe PID: 5240 Parent PID: 3292

General

Start time:	04:17:45
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\iBq\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\iBq\rdpinput.exe
Imagebase:	0x7ff609400000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
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: 00000029.00000002.514047905.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis