JoeSandbox Cloud BASIC

Analysis Report P3FwQWmwUM.exe

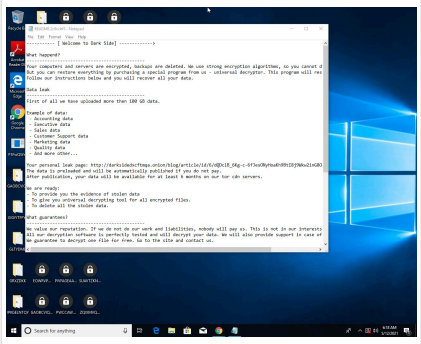
Create Interactive Tour

Overview

General Information

Sample Name:	P3FwQWmwUM.exe
Analysis ID:	411752
MD5:	c4da0137cbb99626f…
SHA1:	a38e9891152755d9…
SHA256:	1d4c0b32aea68056…
Tags:	darkside OASISCOURTLIMITED ransomware signed
Infos:	

Most interesting Screenshot:



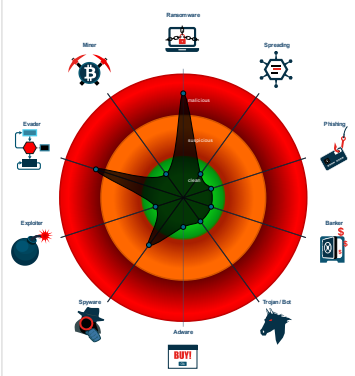
Detection

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

Signatures

- Antivirus / Scanner detection for submitted s…
- Found ransom note / readme
- Multi AV Scanner detection for submitted file
- Yara detected DarkSide Ransomware
- Changes security center settings (notificatio…
- Contains functionality to change the wallpaper
- Found Tor onion address
- Machine Learning detection for sample
- PE file has a writeable .text section
- AV process strings found (often used to ter…
- Abnormal high CPU Usage
- Checks if Antivirus/Antispyware/Firewall pro…
- Contains functionality to access loader funct…
- Contains functionality to call native functions
- Contains functionality to delete services

Classification



Startup

- **System is w10x64**
- P3FwQWmwUM.exe (PID: 5976 cmdline: 'C:\Users\user\Desktop\P3FwQWmwUM.exe' MD5: C4DA0137CBB99626FD44DA707AE1BCA8)
- P3FwQWmwUM.exe (PID: 6020 cmdline: 'C:\Users\user\Desktop\P3FwQWmwUM.exe' MD5: C4DA0137CBB99626FD44DA707AE1BCA8)
  - P3FwQWmwUM.exe (PID: 1600 cmdline: 'C:\Users\user\Desktop\P3FwQWmwUM.exe' MD5: C4DA0137CBB99626FD44DA707AE1BCA8)
    - P3FwQWmwUM.exe (PID: 2900 cmdline: C:\Users\user\Desktop\p3fwqwmwum.exe -work worker0 -path \\?\C:\ MD5: C4DA0137CBB99626FD44DA707AE1BCA8)
- svchost.exe (PID: 5964 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5892 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5408 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3996 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5968 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6248 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6356 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6388 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6076 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5448 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- notepad.exe (PID: 7048 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\README.2c9ccbf3.TXT MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\README.2c9ccbf3.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
C:\README.2c9ccbf3.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
C:\README.2c9ccbf3.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
C:\README.2c9ccbf3.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
C:\README.2c9ccbf3.TXT	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
Click to see the 30 entries				

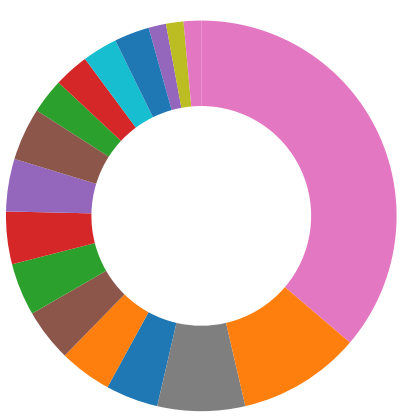
Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.432905231.0000000002DB4000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000004.00000003.362840336.0000000002B69000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000004.00000003.327849253.0000000000849000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	
00000004.00000003.411060522.0000000002D70000.00000004.00000001.sdmp	JoeSecurity_DarkSide	Yara detected DarkSide Ransomware	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

Click to jump to signature section

Show All Signature Results

AV Detection:

Antivirus / Scanner detection for submitted sample	Show sources
Multi AV Scanner detection for submitted file	Show sources
Machine Learning detection for sample	Show sources

Networking:

Found Tor onion address	Show sources

Spam, unwanted Advertisements and Ransom Demands:

Found ransom note / readme	Show sources
Yara detected DarkSide Ransomware	Show sources
Contains functionalty to change the wallpaper	Show sources

System Summary:

PE file has a writeable .text section	Show sources

Lowering of HIPS / PFW / Operating System Security Settings:

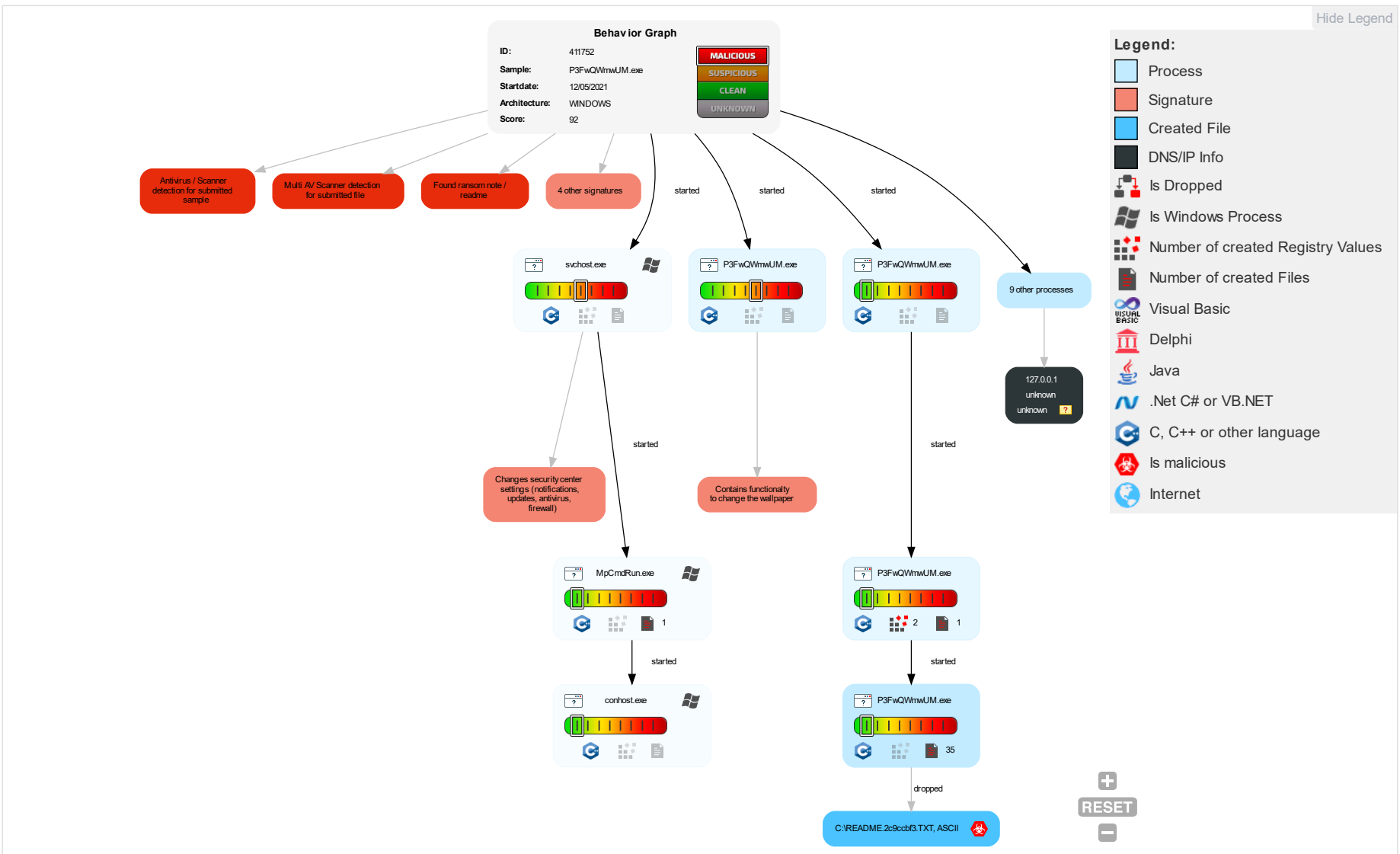
Changes security center settings (notifications, updates, antivirus, firewall)	Show sources

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts 2	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Defacement 1
Default Accounts	Native API 1	Valid Accounts 2	Valid Accounts 2	Obfuscated Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Proxy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	Service Execution 1 2	Windows Service 1 4	Access Token Manipulation 2	Software Packing 2	Security Account Manager	File and Directory Discovery 1 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 1	Windows Service 1 4	DLL Side-Loading 1	NTDS	System Information Discovery 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 2	Masquerading 1 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1	Valid Accounts 2	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 2	Proc Filesystem	Process Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

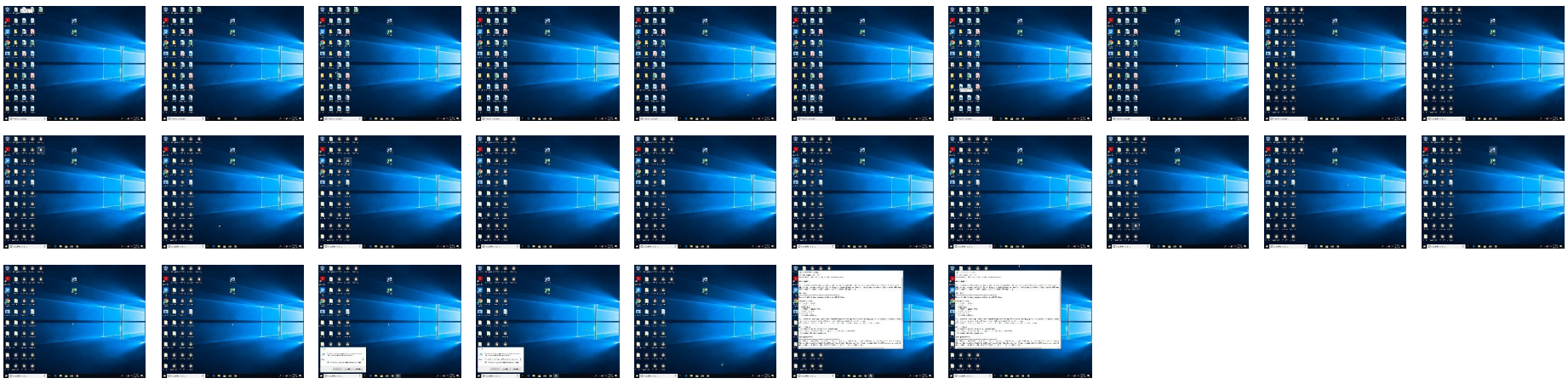
Behavior Graph

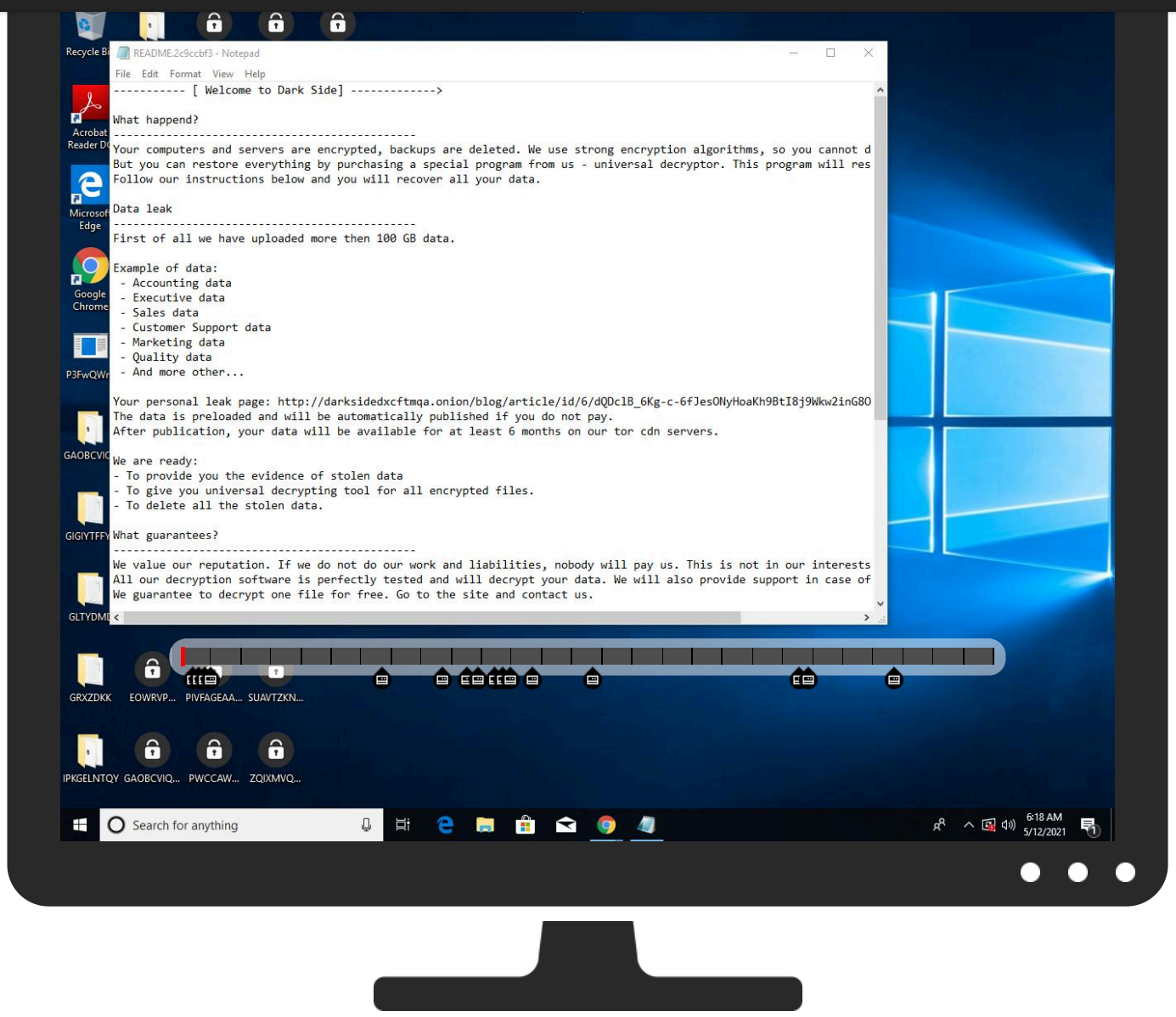


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
P3FwQWmwUM.exe	46%	Virustotal		Browse
P3FwQWmwUM.exe	62%	ReversingLabs	Win32.Ransomware.DarkSide	
P3FwQWmwUM.exe	100%	Avira	TR/Crypt.XPACK.Gen	
P3FwQWmwUM.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.P3FwQWmwUM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://darksidedxcftmqa.onion/blog/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://darksidfqzcuhtk2.onion/K71D6P8	0%	Avira URL Cloud	safe	
https://sectigo.com/CPS0D	0%	URL Reputation	safe	
https://sectigo.com/CPS0D	0%	URL Reputation	safe	
https://sectigo.com/CPS0D	0%	URL Reputation	safe	

http://darksidedxcftmqa.onion/blog/article/	0%	Avira URL Cloud	safe	
http://darksidfqzcuhtk2.onion/K71D6P88YTX04R3ISCJZHMD5IYV55V9D	0%	Avira URL Cloud	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wkw2inG8O72jWaOcKbr	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
https://activity.windows.comr	0%	URL Reputation	safe	
https://activity.windows.comr	0%	URL Reputation	safe	
https://activity.windows.comr	0%	URL Reputation	safe	
https://%s.xboxlive.com	0%	URL Reputation	safe	
https://%s.xboxlive.com	0%	URL Reputation	safe	
https://%s.xboxlive.com	0%	URL Reputation	safe	
http://ocsp.sectigo.com0%	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
https://dynamic.t	0%	URL Reputation	safe	
https://dynamic.t	0%	URL Reputation	safe	
https://dynamic.t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wk	0%	Avira URL Cloud	safe	
https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Download Network PCAP: filtered – full

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411752
Start date:	12.05.2021
Start time:	06:15:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	full
Sample file name:	P3FwQWmwUM.exe
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:	23
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.rans.evad.winEXE@19/47@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 89%) • Quality average: 75.8% • Quality standard deviation: 33.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:16:36	API Interceptor	2x Sleep call for process: svchost.exe modified
06:17:55	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
06:18:05	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\README.2c9ccbf3.TXT

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:\ProgramData\2c9ccbf3.ico Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	MS Windows icon resource - 5 icons, 64x64, 32 bits/pixel, 48x48, 32 bits/pixel
Category:	dropped
Size (bytes):	34494

SSDEEP:	192:gbjP3AIUIsjVX50pzKOMkbD0NY3dlZJJw:8jP3AuIsj7cOTkVlZJW
MD5:	4F57D54D01CCBDAF3EBFAC3EC0AC3FD7
SHA1:	BC529DC03674D08D64D8442C4E1D1A3E3464E953
SHA-256:	28B6841AA125225CD01BE09FBD2F1D7B3C2102D9FFC7DC8546700E67C2A6E3BC
SHA-512:	BA9F779C0066EBEC8E555276AFBC862456B083138F8EB512CAE50B431EBE32C74C0A5EFB4E99F995BCFCBAEC2B71E242984FDD5084561940E741F1CAC1D6C246
Malicious:	false
Preview:	......@@.... .(B..V...00.... ..%..~B.. ....&h........ ......x........ .h...V...(...@......... ......B...222.222.222.222. 222.222.222.222.222.222..222.222.222.222.222.222.222.222.22 2.222.222.222.222.222.222.222.222.222.222.222.222.222...222.....222.222.222.222.22 2.222.222.222.222 222+22222222222+222 222.222.222.222.222.222.222.222.....222...222.222.222. 222.222.222.222.222.222=222v22

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5959966958795487
Encrypted:	false
SSDEEP:	6:b7ZcE2k1GaD0JOCEfMuaaD0JOCEfMKQmDtc9tAl/gz2cE0fMbhEZolrRSQ2hyYl8:b7ZTGaD0JcaaD0JwQQtatAg/0bjSQJ
MD5:	B04CC4E70792D21CB512B58CAB471DF0
SHA1:	47CD1EFFD275EE99A5382319F44966938011144B
SHA-256:	3887596A218A6744507CC827267D24292A690345BA24865FF04D0A9A3C2E6D29
SHA-512:	2D2E82A381D641DD0B57AEA23CA24AADF218DD7CE0B6F10CCF8FC5515EF01AA05B6D599A3E40CB5E56A9BABB767D086D6711083FBDCD0D8AD024FC21C2247AC9
Malicious:	false
Preview:	....E..h..(.....$....y............... ..1C:\ProgramData\Microsoft\Network\Downloader\... ....C:\ProgramData\Microsoft\Network\Downloader\.. ....0u..................@...@..................$....y............&......e.f.3...w......................3...w.................h..C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a .d.e.r.\.q.m.g.r...d.b...G...

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0df7824b, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09569855989648687
Encrypted:	false
SSDEEP:	6:fSZGzwl/+hsNlsRlE11Y8TRX6NyyKJSZGzwl/+hsNlsRlE11Y8TRX6NyyK:yG0+k6O4bl6XK4G0+k6O4bl6XK
MD5:	FD1613636B5C1F0359604709CF7E28D7
SHA1:	0DD34912978CFECFC99094B13606F328245AD3BD
SHA-256:	2C7D8799130967A0D07A9AA42F392C464F8B1BCA5A8E8F6638F62AFE15A08648
SHA-512:	CDAF197A0E12CB998F31C0AEADE714A867F6A4F48018B724A584D6850F809B81F884DBC6BF99221409AA69670C59269B06E6B2D4AF56E7735F2FE8547CA58539
Malicious:	false
Preview:	...K... ....e.f.3...w.......................&..........w..$....y..h.(.............................3...w...B...........@.. ....3...w.. ....;.'.$....y.....................$....y... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10955675807642352
Encrypted:	false
SSDEEP:	3:A09EvB6hl/bJdAtiZlhXall:A5Kt4re
MD5:	5DB88030C44E742C58C02D9BD3CAED65
SHA1:	985AC0D2D0CEB93C055B8FCB35CA703DD4AF7B75
SHA-256:	65783AEA2F43380F918BC71664CF21305EFDE5D453D7A54BBFA76D8887C41FD3
SHA-512:	4ADFFCBAC07EEABF953E7351DAD655AA97D04E77CC2F5A6F77D3DE37A3B31C2CC21518C07AA59619621B660426B7FCFD75075B6EA8B2E01F1277E20788A31231
Malicious:	false
Preview:	*..H..................................3...w..$....y.......w...............w.......w....:O.....w......................$....y.. ....

C:\README.2c9ccbf3.TXT

Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security

- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security
- Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: C:\README.2c9ccbf3.TXT, Author: Joe Security

Preview:	---------- [Welcome to Dark Side] ------------>....What happend?..---..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..---..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.......Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\InputPersonalization\README.2c9ccbf3.TXT

Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60IO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ------------>....What happend?..---..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..---..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.......Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore\README.2c9ccbf3.TXT

Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60IO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ------------>....What happend?..---..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..---..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.......Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\README.2c9ccbf3.TXT

Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60IO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ------------>....What happend?..---..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..---..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.......Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9BtI8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\Gadgets\README.2c9ccbf3.TXT

Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe

Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ----------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ----------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\Windows Sidebar\settings.ini.2c9ccbf3 Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	7.0704859487274
Encrypted:	false
SSDEEP:	6:BPPEkTtpcbnYmM7E1cFw4aQmW5C8QVPbn4WEk/mxINL5:B33tp8nVM7E1Kz5c3xQxz5
MD5:	07E2AE220FFCB84C5D8EE4A7461F29B7
SHA1:	F16D1AD28BB5FF13FEE295A2F8C74908A563A710
SHA-256:	326EBC5FCCCF17C7546D1E45062D7E06653DB9640A02174E6A0BDC3BBA9FE7B9
SHA-512:	D32E1607BD37F7D20DF79DC8D1CCCB7593D65E90771C04F4DE660C0570A85CA4DAEF1F5D703428919F6934DF72AD35BB0B2B6A4D52166D258A92D69A8CE24E1E
Malicious:	false
Preview:	'.....*W.m....x.v....g.....:V.H*u?..| .....{}.....w:.nK.6C2.f.3.W.....8..`.XB.c..g+....3.....z.....+A9.....i.2..\..L.9"9...\Bf.q5w.Z:.+3.hv.....i.....?.IV...'Qw7..(.(.a..DI...D..x.I....~....h.Ya..

C:\Users\Default\AppData\Local\Microsoft\WindowsApps\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ----------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\Windows\History\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ----------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and

C:\Users\Default\AppData\Local\Microsoft\Windows\INetCache\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Microsoft\Windows\INetCookies\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Local\Temp\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Network Shortcuts\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false

SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Printer Shortcuts\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDcIB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Compressed (zipped) Folder.ZFSendToTarget.2c9ccbf3 Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	data
Category:	dropped
Size (bytes):	147
Entropy (8bit):	6.702940712124431
Encrypted:	false
SSDEEP:	3:K/WR6TulDWAzALewzTaEegpCKxfqXjeM8wYkdduvqENn:K/WR6TqWOae2aEesCGfKjt8w0iEN
MD5:	16C0DF9DBF28481841509F41E09CD06B
SHA1:	EBF28D457E93919F0B1674059CF71FF2CC74987B
SHA-256:	AE8EF7770A41C8F02DE986351CA2CE7BAC80C6A5730ADF3E0FAA72A30BB1D72B
SHA-512:	DE900308B5E2120EF9C3A4D02FF59B206B810812E9474DB972CAF4B59913EB45C21F01AD2FD985A7E7C2426B5E382760BFB1964925487B9524B572743399E6C6
Malicious:	false
Preview:	...).Fs.I.....V.B..@...4.'D..Y.S...S..B!.....we6x=../..I.L.g16.s..8.$)G.8..7...d.....w.n.....u.9.;....)+3..r[.....3.._...o.;.p..[7. ..

C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Mail Recipient.MAPIMail.2c9ccbf3 Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	6.738004463528832
Encrypted:	false
SSDEEP:	3:HGtr9OsqDGxO9NPnS7WeAWVu0CL2KM7i+ZZNlOp7gHPV5UpJ5elsduF4ZB:O9Os3IfIWeASpKM7i+nNlY78VukqF+B
MD5:	7B8ABA0DC762B20DD9C6D5D32AD23271
SHA1:	7AA22AABE4A00C15580781DBF48EE119A47E4228
SHA-256:	527899539201C1911FC59D2028BC5428EFA934E84CA43FC278390050112A5D4D
SHA-512:	AFA84F55D86CCEB19DAF0B84216E94A93462C9D03EF6CF766EC7AE83F4E8D9DB8C4201E0EA5D75A26E1D9C60976070362D80A69E95CE75DCD34A215D9944FB6C
Malicious:	false
Preview:	..b.a7.s. ,L...k.6l...n{{..|.k.U ....9_S..3~.F^f.&;%.pK.....,..eH.....).0U...Tg...>.^..-../.2z.#....K.hX..aPf\.QK.Z.p.8g...a.R.....L..

C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so

w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\AppData\Roaming\Microsoft\Windows\Templates\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Desktop\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788

MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Documents\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5340
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	96:LwmxqbMcpdlO/LFz88QMs88XmxqbMcpdlO/LFz88QMs88W:8m0wcpdlOjFz2rbXm0wcpdlOjFz2rbW
MD5:	8B4B7351CE1BEC0085228C2BDA959D4E
SHA1:	7E38648E50AEBD99EB786C1EC68242DB775536DB
SHA-256:	F907D383D6FC3D3C139BBDB97AA34167D2FA185008F402035D4AF20672AA0819
SHA-512:	FE3F944F4A9760DB7E9D0B6C9D56A7CAF6AA691D2749DDD081A71255114BAA584BBE5F2AA7B096CAA3542E61491F38EA7B8DC42D393624EF323E977716261297
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Downloads\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Favorites\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Links\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. -

C:\Users\Default\Music\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	8010
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	192:8m0wcpdlOjFz2rbXm0wcpdlOjFz2rbXm0wcpdlOjFz2rbW:8mVcpM2rDmVcpM2rDmVcpM2r6
MD5:	EF2EF1311ED9C8D68B9A8D3DDA11B484
SHA1:	C84F5DBCCBE395002D7A1AD472B19A856DF3279B
SHA-256:	20D546674D92FA53CF8C5BB978D7800385B892158A8BD5B16837285051A31759
SHA-512:	0C429D01BAC389ADD6C155AE53BC8F3307F04AAC695B22AB1EFC77A970EE96382C14D67916CECCBFAF3BFE7C1A0CC9FF708348A1D2471FE3161F5F2FE4E34405
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Pictures\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	8010
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	192:8m0wcpdlOjFz2rbXm0wcpdlOjFz2rbXm0wcpdlOjFz2rbW:8mVcpM2rDmVcpM2rDmVcpM2r6
MD5:	EF2EF1311ED9C8D68B9A8D3DDA11B484
SHA1:	C84F5DBCCBE395002D7A1AD472B19A856DF3279B
SHA-256:	20D546674D92FA53CF8C5BB978D7800385B892158A8BD5B16837285051A31759
SHA-512:	0C429D01BAC389ADD6C155AE53BC8F3307F04AAC695B22AB1EFC77A970EE96382C14D67916CECCBFAF3BFE7C1A0CC9FF708348A1D2471FE3161F5F2FE4E34405
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Saved Games\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\Default\Videos\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	8010
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	192:8m0wcpdlOjFz2rbXm0wcpdlOjFz2rbXm0wcpdlOjFz2rbW:8mVcpM2rDmVcpM2rDmVcpM2r6

SHA-256:	20D546674D92FA53CF8C5BB978D7800385B892158A8BD5B16837285051A31739
SHA-512:	0C429D01BAC389ADD6C155AE53BC8F3307F04AAC695B22AB1EFC77A970EE96382C14D67916CECCBFAF3BFE7C1A0CC9FF708348A1D2471FE3161F5F2FE4E34405
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\README.2c9ccbf3.TXT Download File

Process:	C:\Users\user\Desktop\P3FwQWmwUM.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2670
Entropy (8bit):	5.442341646702788
Encrypted:	false
SSDEEP:	48:L7WVOqZGKQx8NbSSUD4dcKn3p60lO/DXFz8R6VQMsHcXGvGlZ:LwmxqbMcpdlO/LFz88QMs88W
MD5:	00F2E0214E12B6770923B1242DA68A3A
SHA1:	F23FF75FCD924C3D8363279A9F6D18477A228D83
SHA-256:	472D28010651900FF78C3B044603ECD4F8850F867B74E8B5717B051638D4E536
SHA-512:	FE1AFE0A58724364F2064F2EF65B9EEFA758C3953FF5FD7CD84A10CF5A03E39F0DB73C193B57B99F24E290FB8FB8E4BA837D703DE84E9C5373E9D2C92A3448F2
Malicious:	false
Preview:	---------- [Welcome to Dark Side] ---------->....What happend?..----------..Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data...But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network...Follow our instructions below and you will recover all your data.....Data leak..----------..First of all we have uploaded more then 100 GB data.....Example of data:.. - Accounting data.. - Executive data.. - Sales data.. - Customer Support data.. - Marketing data.. - Quality data.. - And more other.....Your personal leak page: http://darksidedxcftmqa.onion/blog/article/id/6/dQDclB_6Kg-c-6fJesONyHoaKh9Btl8j9Wk w2inG8O72jWaOcKbrxMWbPfKrUbHC..The data is preloaded and will be automatically published if you do not pay...After publication, your data will be available for

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1112291448563076
Encrypted:	false
SSDEEP:	12:dGTnVXm/Ey6q99950F3ekXg1Q10nMCldimE8eawHjcDV:M4l68m0cyMCldzE9BHjcJ
MD5:	341E092D7964B551BD2D177177378025
SHA1:	7420DF32C28DD7DC2D287B91141CC06903982149
SHA-256:	322FA1CC037E0272308011407F8DDEEED1529BE7BF21E867F3B91A7AF78BEE51
SHA-512:	64F826E07D9F7F892B59A4965F19C968DB1E8B068B7A3E6D9FFAB3E8C44582D33F4A4BA6036F83F674D51C30763ED0478351F28CFA2639AF32665E23D8452DE0
Malicious:	false
Preview:	.....@... ....q#.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....?`..... .....h.1G.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.f.r.o.n.t.d.e.s.k.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.@... ....#.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11367434056994173
Encrypted:	false
SSDEEP:	12:OCXVXm/Ey6q99950g1miUkXg1Q10nMCldimE8eawHza1miIfXnF:OCX4l68mg1tUcyMCldzE9BHza1tIf3F
MD5:	E99DA09E3D3E1827D56044DF442BA946
SHA1:	D97FC8964E44A7F17BCE19FAAA38F8B5B201EDC4
SHA-256:	664DDC56CDBF4CE847887E9B088395202229EF26F8B341001827B374825C1879
SHA-512:	932B69466710F5A0F25043176EE8F1E4E03568C0F1D9350C1984CF0FF8CE4563EB88D97991ABDAF8B98FC6120CA84ABB5FC80BF11729CE49EE48F992CBD235CC
Malicious:	false
Preview:	....@... .....!.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....?`..... .....a.1G.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.f.r.o.n.t.d.e.s.k.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.@... .....!.....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl Download File

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11360251702902835
Encrypted:	false
SSDEEP:	12:OCVXm/Ey6q99950F1mK21kXg1Q10nMCldimE8eawHza1mKOF:OC4l68mF1i1cyMCldzE9BHza1M
MD5:	B0D195F5FF730ACCC420FC3BB3818917
SHA1:	818BE027C3B361EEE53BC25E1F82C7B093865B58
SHA-256:	88BEA8F9A9229B2BBC6C220AEAD479215BC1D149DABEB63DCA6D93C0970522CA
SHA-512:	F11A693034185B10666208B8300146151866B4F8736B0592267BBC469A12547295A9BADE55C1026A208C65F46D14C748D1AEA7FD4929B185874DCA5643713031
Malicious:	false
Preview:	....@... ....4.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....?`..... ....._S.1G.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.f.r.o.n.t.d.e.s.k.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.@... ...TA.....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp Download File

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

JoeSandbox Cloud BASIC

Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log Download File

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1465789865752596
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rls8PZk9+MlWlLehB4yAq7ejCEs8vl:OaqdmuF3rlX++kWReH4yJ7MN3l
MD5:	83B76B88FB5AD77FC1A88D7CC777B7F1
SHA1:	263FDED0E0A79B31EF917CB34A26CBE099E2D1D1
SHA-256:	531F2D7E42E90E4D05C44463EAFBCC9602EA563B66BDC3881E69E17B222EDFB2
SHA-512:	8B42875798BD84D51B95033BBB118FBA8CD35AE6B7FCAAE0A3803A6F72AF3D3F0EE1ACD5FA53F24685B7C3E0DD622F006CB2F40E66E7D6BBE4B751020A906F68
Malicious:	false
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. W.e.d. .. M.a.y. .. 1.2. .. 2.0.2.1. .0.6.:.1.7.:.5.5.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. M.a.y. .. 1.2. .. 2.0.2.1. .0.6.:.1.7.:.5.5.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.884829006908391
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	P3FwQWmwUM.exe
File size:	61784
MD5:	c4da0137cbb99626fd44da707ae1bca8
SHA1:	a38e9891152755d9e7fff7386bb5a1bca375bd91
SHA256:	1d4c0b32aea68056755daf70689699200ffa09688495ccd65a0907cade18bd2a
SHA512:	dd8212ff73522c6590ff8d8a3a48276fd872649eada2315b045c8c9f6cf054c3fe6cd741a16744eb82eff763acb745f07336c44db8f0c693770180cf7fd90645
SSDEEP:	1536:mWIrgG/4CMjuhy03Z63tFjr5EOkplsT6oKw8ebioQ+9o:ZG/4CJhxIdJr5sDBKw7jo
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...G.,`..................... >....................@..................................>......................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40a30f
Entrypoint Section:	.text1
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x602C1447 [Tue Feb 16 18:51:51 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	f9ade0aa18f660a34a4fa23392e21838

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB

Not Before, Not After	• 12/20/2020 4:00:00 PM 12/21/2021 3:59:59 PM
Subject Chain	• CN=OASIS COURT LIMITED, O=OASIS COURT LIMITED, STREET=10 Stoneleigh Park, L=Colchester, S=Essex, PostalCode=CO3 9FA, C=GB
Version:	3
Thumbprint MD5:	45F07555A52F3B879EEF9866C1947E62
Thumbprint SHA-1:	269F25E6B7C690AE094086BD7825D03B48D4FCB1
Thumbprint SHA-256:	634D08D08A8AE4DBC0A8416DBB49C23DC44257E597DD7C0CB024F5EC41384370
Serial:	00E4E795FD1FD25595B869CE22AA7DC49F

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8393	0x8400	False	0.953480113636	data	7.95739719557	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.text1	0xa000	0x33c	0x400	False	0.5556640625	data	5.47111115827	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0x158	0x200	False	0.384765625	data	2.56207517749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0x39f4	0x3400	False	0.969801682692	data	7.90932575456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0xec9	0x1000	False	0.935546875	data	7.68351864836	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

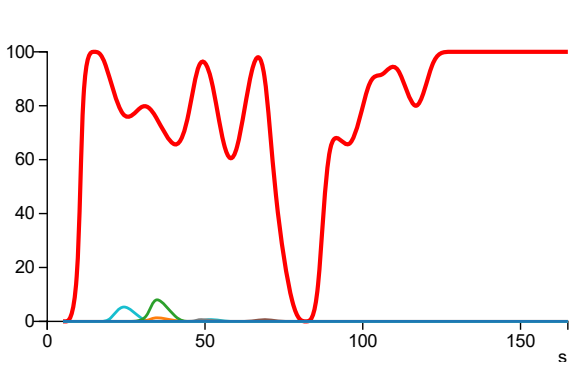
Download Network PCAP: filtered – full

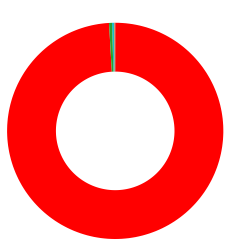
UDP Packets

Code Manipulations

Statistics

CPU Usage

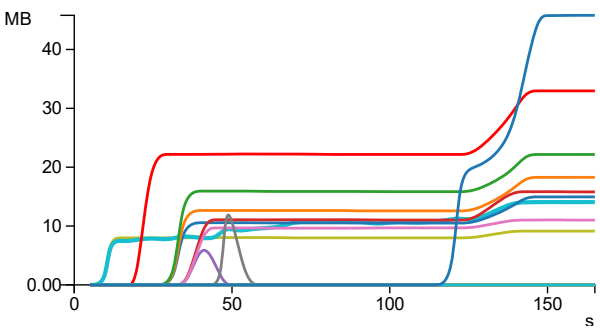


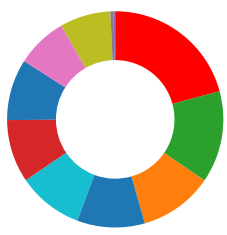


P3FwQWmwUM.exe
P3FwQWmwUM.exe
P3FwQWmwUM.exe
P3FwQWmwUM.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
SgrmBroker.exe
svchost.exe
svchost.exe
MpCmdRun.exe
conhost.exe
notepad.exe

Click to jump to process

Memory Usage

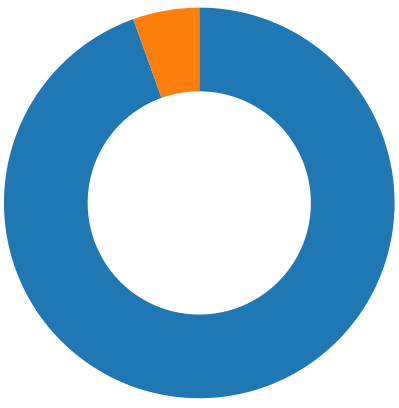




P3FwQWmwUM.exe
P3FwQWmwUM.exe
P3FwQWmwUM.exe
P3FwQWmwUM.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
SgrmBroker.exe
svchost.exe
svchost.exe
MpCmdRun.exe
conhost.exe
notepad.exe

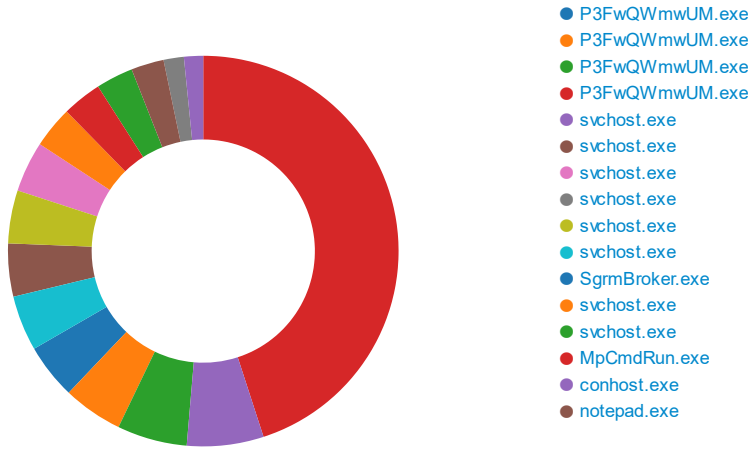
Click to jump to process

High Level Behavior Distribution



Click to dive into process behavior distribution

Behavior



Click to jump to process

System Behavior

Analysis Process: P3FwQWmwUM.exe PID: 5976 Parent PID: 5876

Function Logs

General

Start time:	06:16:23
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\P3FwQWmwUM.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\P3FwQWmwUM.exe'
Imagebase:	0x400000
File size:	61784 bytes
MD5 hash:	C4DA0137CBB99626FD44DA707AE1BCA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000001.00000002.232594392.00000000007AA000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Section Activities

Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities

Show Windows behavior

Key Opened

Key Value Queried

Mutex Activities

Show Windows behavior

Process Activities

Show Windows behavior

Process Terminated

Thread Activities

Show Windows behavior

JoeSandbox Cloud BASIC

Memory Activities — Show Windows behavior

System Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: P3FwQWmwUM.exe PID: 6020 Parent PID: 560

Function Logs

General

Start time:	06:16:24
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\P3FwQWmwUM.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\P3FwQWmwUM.exe'
Imagebase:	0x400000
File size:	61784 bytes
MD5 hash:	C4DA0137CBB99626FD44DA707AE1BCA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000002.00000002.235019158.0000000000537000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Key Opened

Key Value Queried

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Created

Process Terminated

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

Object Security Activities — Show Windows behavior

Security Object Set

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: P3FwQWmwUM.exe PID: 1600 Parent PID: 6020

Function Logs

General

Start time:	06:16:24
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\P3FwQWmwUM.exe

Imagebase:	0x400000
File size:	61784 bytes
MD5 hash:	C4DA0137CBB99626FD44DA707AE1BCA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000003.00000002.509189468.00000000004F8000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Key Opened

Key Created

Key Value Created

Key Value Queried

Mutex Activities — Show Windows behavior

Mutex Created

Process Activities — Show Windows behavior

Process Created

Thread Activities — Show Windows behavior

Thread Execution Resumed

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Process Token Activities — Show Windows behavior

Token Adjusted

Object Security Activities — Show Windows behavior

Security Object Set

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: P3FwQWmwUM.exe PID: 2900 Parent PID: 1600 — Function Logs

General

Start time:	06:16:25
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\P3FwQWmwUM.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\p3fwqwmwum.exe -work worker0 -path \\?\C:\
Imagebase:	0x400000
File size:	61784 bytes

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.432905231.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.362840336.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.327849253.0000000000849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411060522.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.408654426.0000000002B6A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.236181936.00000000007C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.435986395.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.337715138.0000000002B07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.299389052.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000002.516574687.0000000002DA2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.478288044.0000000002AB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.282398886.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.303767851.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.439503040.0000000002AB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.298944879.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.307244631.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.442911884.0000000002E08000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.295652654.0000000002AA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.428084952.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.288394609.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.408145616.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.330427301.0000000000849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.306781726.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.292805057.0000000002A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.281893608.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.483773853.0000000002E39000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.297343335.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.282524954.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.433763245.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.288157426.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411401825.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.321471581.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.436219840.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.282409788.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.430404279.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411544467.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.432232782.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.474609577.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.407959058.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.429585276.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.328363880.0000000000849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.236245311.00000000007C8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411912846.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.302439227.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.290040157.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.307472011.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.443960653.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.353326118.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000002.516426859.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.362876492.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.433058006.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.288198091.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.434687514.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.328783962.0000000000849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.279059079.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411798869.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.293724321.0000000002A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000002.510936905.0000000000768000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.408432832.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.456394908.0000000002AB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.347522767.0000000002AA7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.409934886.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.411159789.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.410791890.0000000002B4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.447874704.0000000002AB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.337437975.0000000002B07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.433675898.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.431227855.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.408616972.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.428965052.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.307770705.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.288409928.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.348924422.0000000002AA7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.280790972.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.280803963.000000000084D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.492039293.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.440558230.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.294802191.0000000002AA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.440164319.0000000002AB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.353303558.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.304436022.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.428206439.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.443023882.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.293143940.0000000002A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.432131880.0000000002DB4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.409798220.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.428389024.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.289927003.000000000084C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.328127290.0000000000849000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.493025969.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.368476921.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.429695025.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.448359001.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.304226241.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.483856895.0000000002D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.293461617.0000000002A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.410319943.0000000002B4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.410677619.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.349425661.0000000002AA7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.321323465.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.311791138.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.337762957.0000000002B07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.409162945.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.434752909.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.302198707.00000000007F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.415423650.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.410205898.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.473912941.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.479859917.0000000002E18000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.439469384.0000000002E08000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.295417556.0000000002AA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.456833891.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.294724805.0000000002AA0000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.409597850.0000000002B69000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.431347630.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.409312887.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.441657546.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.430481720.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.415984076.0000000002B47000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.458381849.0000000002D60000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.415652999.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.336753706.0000000002B07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.408806702.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000004.00000003.281911971.000000000084D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

- File Opened
- File Created
- File Moved
- File Written
- File Read
- File Attributes Queried
- Other File Operations

Section Activities — Show Windows behavior

- Sections loaded by Windows
- Sections loaded by Program

Registry Activities — Show Windows behavior

- Key Opened
- Key Value Queried

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

- Process Information Set

Thread Activities — Show Windows behavior

- Thread Created

Memory Activities — Show Windows behavior

- Memory Usage Statistics

System Activities — Show Windows behavior

Process Token Activities — Show Windows behavior

- Token Adjusted

Object Security Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 5964 Parent PID: 560

Function Logs

General

Start time:	06:16:36
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000

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

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 5892 Parent PID: 560

Function Logs

General

Start time:	06:16:46
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 5408 Parent PID: 560

Function Logs

General

Start time:	06:16:48
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 3996 Parent PID: 560

Function Logs

General

Start time:	06:16:48

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 5968 Parent PID: 560

Function Logs

General

Start time:	06:16:50
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 6248 Parent PID: 560

Function Logs

General

Start time:	06:16:50
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: SgrmBroker.exe PID: 6356 Parent PID: 560

Function Logs

General

Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff780c50000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Thread Activities — Show Windows behavior

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

Timing Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 6388 Parent PID: 560

Function Logs

General

Start time:	06:16:52
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

COM Activities — Show Windows behavior

WMI Operations

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: svchost.exe PID: 6664 Parent PID: 560

Function Logs

General

Start time:	06:17:01
Start date:	12/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Section Activities — Show Windows behavior

Sections loaded by Windows

Sections loaded by Program

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

System Information Queried

Timing Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: MpCmdRun.exe PID: 6076 Parent PID: 6388

Function Logs

General

Start time:	06:17:53
Start date:	12/05/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7ab9a0000
File size:	455656 bytes

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Opened

File Written

File Attributes Queried

Other File Operations

Section Activities — Show Windows behavior

Sections loaded by Windows

Registry Activities — Show Windows behavior

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Queried

Process Information Set

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Usage Statistics

System Activities — Show Windows behavior

Language or Locale ID Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: conhost.exe PID: 5448 Parent PID: 6076

Function Logs

General

Start time:	06:17:55
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Attributes Queried

Volume Information Queried

Section Activities — Show Windows behavior

Sections loaded by Windows

Mutex Activities — Show Windows behavior

Mutex Created

Process Activities — Show Windows behavior

Thread Activities — Show Windows behavior

Thread Created

Thread Delayed

System Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Window Created

Message Posted to Windows UI

Window UIs Event Hook Set

LPC Port Activities — Show Windows behavior

Chronological Activities

Analysis Process: notepad.exe PID: 7048 Parent PID: 3292

Function Logs

General

Start time:	06:18:14
Start date:	12/05/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\README.2c9ccbf3.TXT
Imagebase:	0x7ff6a7f60000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DarkSide, Description: Yara detected DarkSide Ransomware, Source: 00000016.00000002.505242943.0000019FB6B02000.00000004.00000020.sdmp, Author: Joe Security

File Activities — Show Windows behavior

File Opened

Section Activities — Show Windows behavior

Sections loaded by Windows

Registry Activities — Show Windows behavior

Key Opened

Key Value Queried

Mutex Activities — Show Windows behavior

Process Activities — Show Windows behavior

Process Queried

Thread Activities — Show Windows behavior

Thread Information Set

Memory Activities — Show Windows behavior

Memory Allocated

Memory Usage Statistics

System Information Queried

Timing Activities — Show Windows behavior

Windows UI Activities — Show Windows behavior

Window Created

Window UI Enumerated

Message Posted to Windows UI

LPC Port Activities — Show Windows behavior

Chronological Activities

Disassembly

Code Analysis

Analysis Process: P3FwQWmwUM.exe PID: 5976 Parent PID: 5876 P3FwQWmwUM.exe COMMON

Executed Functions

Function 0040911D, Relevance: 21.2, APIs: 11, Strings: 1, Instructions: 179 HDC COMMON — Download Yara Rule

Function 00401EBC, Relevance: 15.1, APIs: 10, Instructions: 103 HDC NATIVE MEMORY COMMON — Download Yara Rule

Function 00401D45, Relevance: 9.1, APIs: 6, Instructions: 72 HDC REGISTRY MEMORY NATIVE COMMON — Download Yara Rule

Function 004026A6, Relevance: 7.5, APIs: 5, Instructions: 46 HDC SERVICE COMMON — Download Yara Rule

Function 00402742, Relevance: 7.5, APIs: 5, Instructions: 32 HDC SERVICE COMMON — Download Yara Rule

Function 00401867, Relevance: 3.0, APIs: 2, Instructions: 47 HDC LIBRARY LOADER COMMON — Download Yara Rule

Function 00402A44, Relevance: 58.0, APIs: 32, Strings: 1, Instructions: 291 HDC MEMORY STRING COMMON — Download Yara Rule

Function 00401E1B, Relevance: 1.6, APIs: 1, Instructions: 64 HDC COMMON — Download Yara Rule

Function 0040A30F, Relevance: 1.5, APIs: 1, Instructions: 10 HDC COMMON — Download Yara Rule

Non-executed Functions

Function 004033B9, Relevance: 72.2, APIs: 38, Strings: 3, Instructions: 439 HDC MEMORY NATIVE COMMON — Download Yara Rule

Function 00408BD6, Relevance: 47.5, APIs: 22, Strings: 5, Instructions: 231 HDC MEMORY NATIVE THREAD COMMON — Download Yara Rule

Function 00405E35, Relevance: 42.2, APIs: 22, Strings: 2, Instructions: 199 HDC MEMORY NATIVE FILE COMMON — Download Yara Rule

Function 0040409F, Relevance: 36.9, APIs: 20, Strings: 1, Instructions: 133 HDC MEMORY FILE COMMON — Download Yara Rule

Function 00407784, Relevance: 36.3, APIs: 24, Instructions: 278 HDC MEMORY COMMON — Download Yara Rule

Function 004056D4, Relevance: 36.2, APIs: 24, Instructions: 214 HDC MEMORY NATIVE COMMON — Download Yara Rule

Function 004066AC, Relevance: 33.5, APIs: 18, Strings: 1, Instructions: 220 HDC MEMORY FILE COMMON — Download Yara Rule

Function 00406EB7, Relevance: 30.2, APIs: 20, Instructions: 203 HDC MEMORY COMMON — Download Yara Rule

Function 00406C06, Relevance: 29.9, APIs: 15, Strings: 2, Instructions: 180 HDC PROCESS MEMORY NATIVE COMMON — Download Yara Rule

Function 004039E3, Relevance: 27.1, APIs: 18, Instructions: 146 HDC MEMORY REGISTRY NATIVE COMMON — Download Yara Rule

Function 00407B27, Relevance: 24.7, APIs: 13, Strings: 1, Instructions: 164 HDC MEMORY NATIVE COMMON — Download Yara Rule

Function 004027BC, Relevance: 24.6, APIs: 13, Strings: 1, Instructions: 134 HDC NATIVE REGISTRY PROCESS COMMON — Download Yara Rule

Function 0040456A, Relevance: 22.8, APIs: 12, Strings: 1, Instructions: 96 HDC MEMORY COMMON — Download Yara Rule

Function 0040625C, Relevance: 18.1, APIs: 12, Instructions: 120 HDC MEMORY NATIVE COMMON — Download Yara Rule

Function 00407D8B, Relevance: 16.6, APIs: 11, Instructions: 120 HDC MEMORY COMMON	Download Yara Rule
Function 004046E2, Relevance: 16.6, APIs: 11, Instructions: 102 HDC SERVICE MEMORY COMMON	Download Yara Rule
Function 00401B91, Relevance: 15.8, APIs: 8, Strings: 1, Instructions: 76 HDC MEMORY FILE COMMON	Download Yara Rule
Function 00405C1C, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 126 HDC FILE NATIVE NETWORK COMMON	Download Yara Rule
Function 004069E1, Relevance: 13.6, APIs: 9, Instructions: 98 HDC NATIVE THREAD SLEEP COMMON	Download Yara Rule
Function 00408016, Relevance: 13.6, APIs: 9, Instructions: 93 HDC MEMORY REGISTRY NATIVE COMMON	Download Yara Rule
Function 00404878, Relevance: 12.1, APIs: 8, Instructions: 92 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 0040318A, Relevance: 10.6, APIs: 7, Instructions: 98 HDC NATIVE COMMON	Download Yara Rule
Function 00408249, Relevance: 10.6, APIs: 7, Instructions: 95 HDC MEMORY REGISTRY NATIVE COMMON	Download Yara Rule
Function 00408160, Relevance: 10.6, APIs: 7, Instructions: 74 HDC MEMORY REGISTRY NATIVE COMMON	Download Yara Rule
Function 00402160, Relevance: 10.6, APIs: 7, Instructions: 70 HDC NATIVE MEMORY COMMON	Download Yara Rule
Function 00403FBA, Relevance: 10.6, APIs: 7, Instructions: 68 HDC FILE COMMON	Download Yara Rule
Function 00405564, Relevance: 9.1, APIs: 6, Instructions: 96 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 00405756, Relevance: 9.1, APIs: 6, Instructions: 85 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 00405778, Relevance: 9.1, APIs: 6, Instructions: 85 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 00403EDD, Relevance: 9.1, APIs: 6, Instructions: 70 HDC FILE COMMON	Download Yara Rule
Function 004020A3, Relevance: 9.1, APIs: 6, Instructions: 69 NATIVE MEMORY COMMON	Download Yara Rule
Function 00403303, Relevance: 9.1, APIs: 6, Instructions: 66 NATIVE MEMORY COMMON	Download Yara Rule
Function 00408F5B, Relevance: 9.1, APIs: 6, Instructions: 62 HDC FILE NATIVE COMMON	Download Yara Rule
Function 004048D8, Relevance: 7.6, APIs: 5, Instructions: 59 HDC NATIVE MEMORY COMMON	Download Yara Rule
Function 004048B6, Relevance: 7.6, APIs: 5, Instructions: 59 HDC NATIVE MEMORY COMMON	Download Yara Rule
Function 004072E0, Relevance: 7.6, APIs: 5, Instructions: 58 HDC THREAD NATIVE SYNCHRONIZATION COMMON	Download Yara Rule
Function 004054E0, Relevance: 7.5, APIs: 5, Instructions: 48 HDC THREAD NATIVE SYNCHRONIZATION COMMON	Download Yara Rule
Function 00409042, Relevance: 7.1, APIs: 3, Strings: 1, Instructions: 52 HDC NATIVE THREAD COMMON	Download Yara Rule
Function 00401AE1, Relevance: 7.0, APIs: 3, Strings: 1, Instructions: 47 HDC NATIVE THREAD COMMON	Download Yara Rule
Function 00402003, Relevance: 6.1, APIs: 4, Instructions: 60 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 0040221B, Relevance: 6.1, APIs: 4, Instructions: 54 HDC COMMON	Download Yara Rule
Function 00407EFB, Relevance: 6.0, APIs: 4, Instructions: 50 HDC MEMORY COMMON	Download Yara Rule
Function 004055D1, Relevance: 4.5, APIs: 3, Instructions: 46 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 004055AB, Relevance: 4.5, APIs: 3, Instructions: 46 HDC MEMORY NATIVE COMMON	Download Yara Rule
Function 00401C9B, Relevance: 4.5, APIs: 3, Instructions: 41 HDC FILE NATIVE COMMON	Download Yara Rule
Function 00407D2C, Relevance: 4.5, APIs: 3, Instructions: 37 HDC NATIVE SYNCHRONIZATION COMMON	Download Yara Rule
Function 00402E44, Relevance: 3.1, APIs: 2, Instructions: 142 NATIVE COMMON	Download Yara Rule
Function 00403E86, Relevance: 3.0, APIs: 2, Instructions: 37 HDC COMMON	Download Yara Rule
Function 00405CC1, Relevance: 3.0, APIs: 2, Instructions: 32 HDC FILE NATIVE COMMON	Download Yara Rule
Function 004022D9, Relevance: 3.0, APIs: 2, Instructions: 28 HDC NATIVE COMMON	Download Yara Rule
Function 00404A88, Relevance: 1.6, Strings: 1, Instructions: 337 HDC COMMON CRYPTO	Download Yara Rule
Function 00402FB6, Relevance: 1.5, APIs: 1, Instructions: 33 HDC NATIVE COMMON	Download Yara Rule

Function 004054BB, Relevance: 1.5, APIs: 1, Instructions: 14 HDC FILE NATIVE COMMON	Download Yara Rule
Function 00402A1F, Relevance: 1.5, APIs: 1, Instructions: 10 HDC COMMON	Download Yara Rule
Function 004016D2, Relevance: .1, Instructions: 85 HDC COMMON	Download Yara Rule
Function 004017AE, Relevance: .1, Instructions: 76 HDC COMMON	Download Yara Rule
Function 0040A288, Relevance: .0, Instructions: 13 HDC COMMON	Download Yara Rule
Function 004085B7, Relevance: 49.3, APIs: 24, Strings: 4, Instructions: 251 HDC MEMORY NETWORK COMMON	Download Yara Rule
Function 004083CA, Relevance: 31.6, APIs: 21, Instructions: 140 HDC MEMORY COMMON	Download Yara Rule
Function 00407380, Relevance: 24.3, APIs: 16, Instructions: 281 MEMORY COMMON	Download Yara Rule
Function 004063FB, Relevance: 21.1, APIs: 11, Strings: 1, Instructions: 62 HDC MEMORY STRING COMMON	Download Yara Rule
Function 00408995, Relevance: 19.3, APIs: 10, Strings: 1, Instructions: 76 HDC MEMORY STRING COMMON	Download Yara Rule
Function 0040428D, Relevance: 16.7, APIs: 11, Instructions: 216 MEMORY COMMON	Download Yara Rule
Function 00403D8F, Relevance: 15.1, APIs: 10, Instructions: 68 HDC MEMORY COMMON	Download Yara Rule
Function 00408A8E, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 102 HDC MEMORY COMMON	Download Yara Rule
Function 004024C1, Relevance: 14.1, APIs: 7, Strings: 1, Instructions: 62 HDC MEMORY COMMON	Download Yara Rule
Function 00407153, Relevance: 12.1, APIs: 8, Instructions: 72 HDC MEMORY COMMON	Download Yara Rule
Function 00407445, Relevance: 9.1, APIs: 6, Instructions: 104 MEMORY COMMON	Download Yara Rule
Function 0040743A, Relevance: 9.1, APIs: 6, Instructions: 104 MEMORY COMMON	Download Yara Rule
Function 00403BB0, Relevance: 9.1, APIs: 6, Instructions: 104 HDC MEMORY COMMON	Download Yara Rule
Function 00406B24, Relevance: 9.1, APIs: 6, Instructions: 62 HDC MEMORY COMMON	Download Yara Rule
Function 0040611D, Relevance: 6.1, APIs: 4, Instructions: 89 COMMON	Download Yara Rule
Function 00402581, Relevance: 6.1, APIs: 4, Instructions: 55 HDC MEMORY COMMON	Download Yara Rule
Function 00405DC0, Relevance: 6.0, APIs: 4, Instructions: 48 MEMORY COMMON	Download Yara Rule
Function 004064CC, Relevance: 6.0, APIs: 4, Instructions: 45 HDC COMMON	Download Yara Rule
Function 00407F99, Relevance: 6.0, APIs: 4, Instructions: 43 HDC MEMORY COMMON	Download Yara Rule
Function 00402627, Relevance: 6.0, APIs: 4, Instructions: 41 HDC SERVICE COMMON	Download Yara Rule
Function 0040314C, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 26 HDC MEMORY COMMON	Download Yara Rule
Function 00408C93, Relevance: 5.3, APIs: 2, Strings: 1, Instructions: 20 HDC MEMORY NETWORK COMMON	Download Yara Rule