ID: 534013
Sample Name:
dxEOMYaOtV.exe
Cookbook: default.jbs
Time: 00:29:26
Date: 05/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

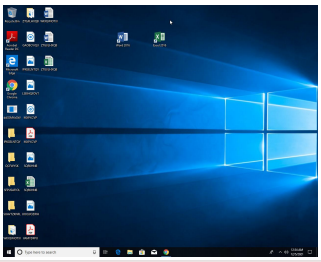
Windows Analysis Report dxEOMYaOtV.exe

Overview

General Information

Sample Name:	dxEOMYaOtV.exe
Analysis ID:	534013
MD5:	a20a44e2add8f2e.
SHA1:	bf2886c5bda80c2..
SHA256:	87b9a82fa050196.
Tags:	exe njrat RAT
Infos:	

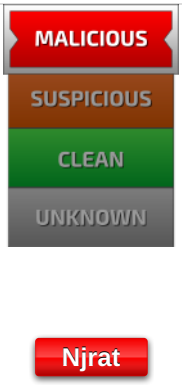
Most interesting Screenshot:



Errors

- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database
- Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service
- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP
- Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog
- Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell Web Request
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Detection



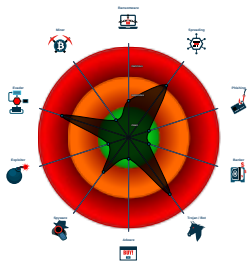
Njrat

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Uses netsh to modify the Windows n…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Modifies the windows firewall
- Contains functionality to spread to U…
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Antivirus or Machine Learning detec…
- May sleep (evasive loops) to hinder …
- May infect USB drives
- Detected potential crypto function
- Sample execution stops while proce…
- Abnormal high CPU Usage
- Enables debug privileges
- Creates a DirectInput object (often fo…
- Found a high number of Window / Us…
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- dxEOMYaOtV.exe (PID: 7008 cmdline: "C:\Users\user\Desktop\dxEOMYaOtV.exe" MD5: A20A44E2ADD8F2EE2434258A20AC815E)
  - netsh.exe (PID: 7096 cmdline: netsh firewall add allowedprogram "C:\Users\user\Desktop\dxEOMYaOtV.exe" "dxEOMYaOtV.exe" ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
    - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Njrat

```
{
  "Campaign ID": "HacKed",
  "Version": "0.7d",
  "Install Name": "3f0e7e396c4b65a76b6471f1f9d6d90a",
  "Install Dir": "Adobe Update",
  "Registry Value": "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
  "Host": "SoftwareMicrosoftWindowsCurrentVersionRun",
  "Port": "NDQz",
  "Network Seprator": "|'|'|"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
dxEOMYaOtV.exe	MAL_Winnti_Sample_May18_1	Detects malware sample from Burning Umbrella report - Generic Winnti Rule	Florian Roth	• 0x13292:$s1: wireshark • 0x1325c:$s2: procexp
dxEOMYaOtV.exe	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x15ca9:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x137c2:$s1: winmgmts:\\.\root\SecurityCenter2 • 0x15717:$s3: Executed As • 0x124f0:$s5: Stub.exe • 0x156f9:$s6: Download ERROR • 0x13784:$s8: Select * From AntiVirusProduct
dxEOMYaOtV.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
dxEOMYaOtV.exe	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x15a57:$reg: SEE_MASK_NOZONECHECKS • 0x156dd:$msg: Execute ERROR • 0x15731:$msg: Execute ERROR • 0x15ca9:$ping: cmd.exe /c ping 0 -n 2 & del

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1182843286.00000000003B2000.00000002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000000.00000002.1182843286.00000000003B2000.00000002.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x15857:$reg: SEE_MASK_NOZONECHECKS • 0x154dd:$msg: Execute ERROR • 0x15531:$msg: Execute ERROR • 0x15aa9:$ping: cmd.exe /c ping 0 -n 2 & del
00000000.00000000.656185698.00000000003B2000.00000002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000000.00000000.656185698.00000000003B2000.00000002.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x15857:$reg: SEE_MASK_NOZONECHECKS • 0x154dd:$msg: Execute ERROR • 0x15531:$msg: Execute ERROR • 0x15aa9:$ping: cmd.exe /c ping 0 -n 2 & del
00000000.00000002.1183435675.00000000029B1000.00000004.00000001.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.dxEOMYaOtV.exe.3b0000.0.unpack	MAL_Winnti_Sample_May18_1	Detects malware sample from Burning Umbrella report - Generic Winnti Rule	Florian Roth	• 0x13292:$s1: wireshark • 0x1325c:$s2: procexp
0.0.dxEOMYaOtV.exe.3b0000.0.unpack	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x15ca9:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x137c2:$s1: winmgmts:\\.\root\SecurityCenter2 • 0x15717:$s3: Executed As • 0x124f0:$s5: Stub.exe • 0x156f9:$s6: Download ERROR • 0x13784:$s8: Select * From AntiVirusProduct
0.0.dxEOMYaOtV.exe.3b0000.0.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0.0.dxEOMYaOtV.exe.3b0000.0.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x15a57:$reg: SEE_MASK_NOZONECHECKS • 0x156dd:$msg: Execute ERROR • 0x15731:$msg: Execute ERROR • 0x15ca9:$ping: cmd.exe /c ping 0 -n 2 & del

Source	Rule	Description	Author	Strings
0.2.dxEOMYaOtV.exe.3b0000.0.unpack	MAL_Winnti_Sample_May 18_1	Detects malware sample from Burning Umbrella report - Generic Winnti Rule	Florian Roth	• 0x13292:$s1: wireshark • 0x1325c:$s2: procexp
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Netsh Port or Application Allowed

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Spreading:

Contains functionality to spread to USB devices (.Net source)

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Njrat

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected Njrat

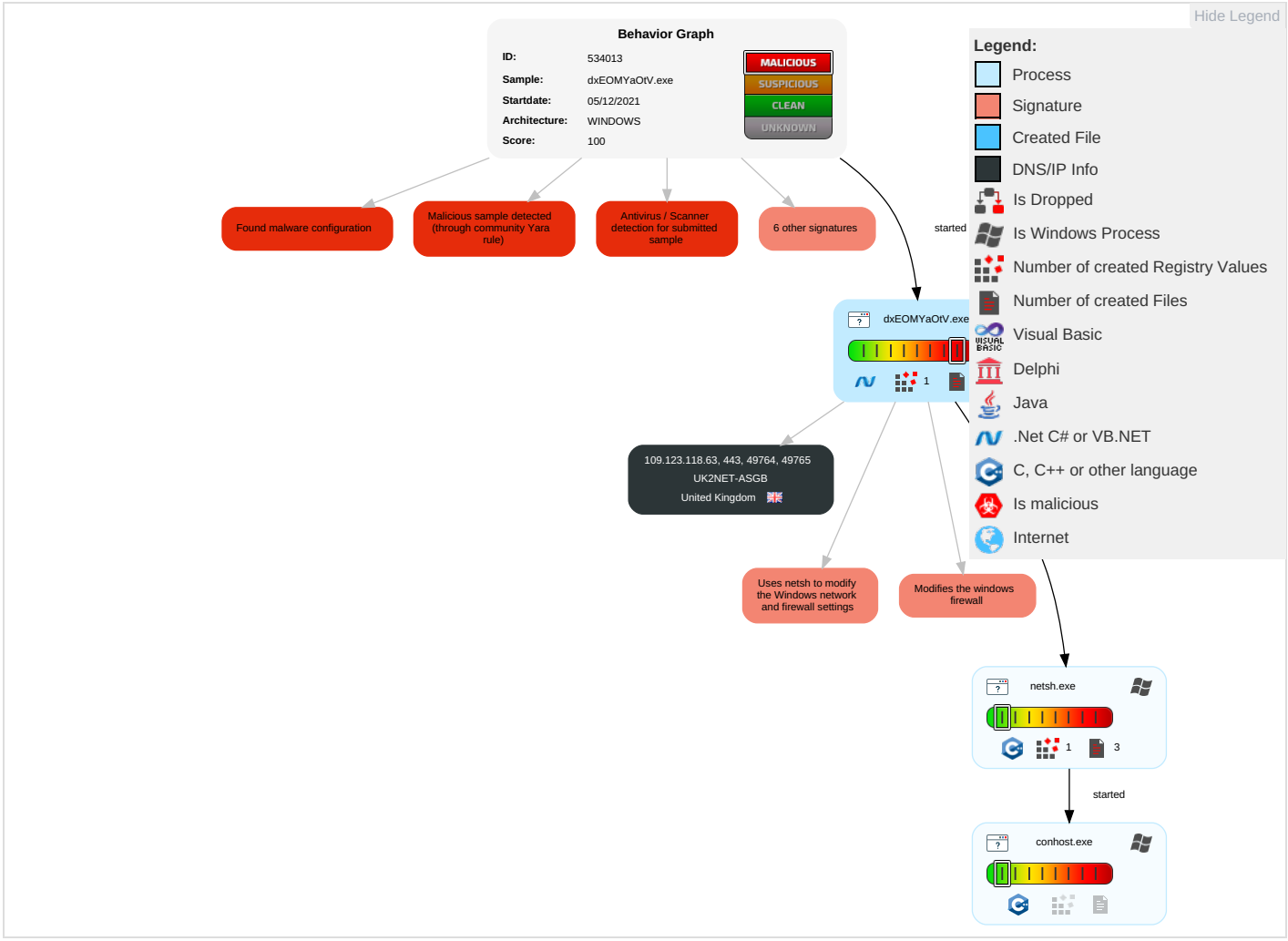
Remote Access Functionality:

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media 1 1	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	Input Capture 1	Security Software Discovery 1	Replication Through Removable Media 1 1	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2	LSA Secrets	Peripheral Device Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

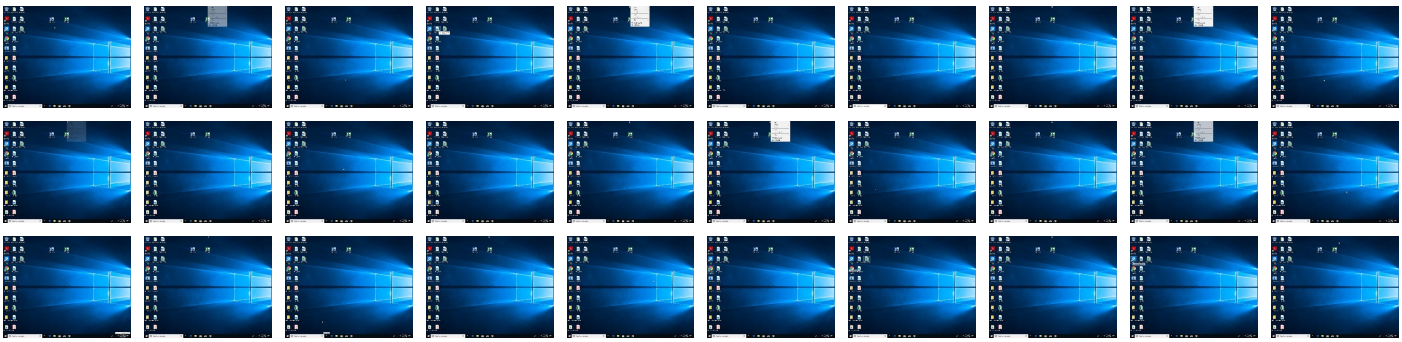
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dxEOMYaOtV.exe	66%	Virustotal		Browse
dxEOMYaOtV.exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
dxEOMYaOtV.exe	100%	Avira	TR/Dropper.Gen	
dxEOMYaOtV.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.dxEOMYaOtV.exe.3b0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.dxEOMYaOtV.exe.3b0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.microsoft.	0%	URL Reputation	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
SoftwareMicrosoftWindowsCurrentVersionRun	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
SoftwareMicrosoftWindowsCurrentVersionRun	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.123.118.63	unknown	United Kingdom		13213	UK2NET-ASGB	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	534013
Start date:	05.12.2021
Start time:	00:29:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dxEOMYaOtV.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.troj.evad.winEXE@4/2@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.2%) • Quality average: 36.6% • Quality standard deviation: 35.4%

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All
Errors:	• Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database • Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service • Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP • Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog • Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell SAM Copy • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UK2NET-ASGB	iEChGuO0Wy.exe	Get hash	malicious	Browse	• 37.123.118.150
	ZDSWrJbftX.exe	Get hash	malicious	Browse	• 37.123.118.150
	Purchase Order.exe	Get hash	malicious	Browse	• 37.123.118.150
	Invoice.exe	Get hash	malicious	Browse	• 37.123.118.150
	Poh Tiong Trading - products list.exe	Get hash	malicious	Browse	• 37.123.118.150
	yMznKPLZVR.exe	Get hash	malicious	Browse	• 37.123.118.150
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 37.123.118.150
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 37.123.118.150
	ENQ 6205009033-6000003867.exe	Get hash	malicious	Browse	• 37.123.118.150
	77isbA5bpi.exe	Get hash	malicious	Browse	• 37.123.118.150
	RTfEx2KIxu	Get hash	malicious	Browse	• 77.92.90.80
	OlHeE02x0N.exe	Get hash	malicious	Browse	• 37.123.118.150
	TT COPY_02101011.exe	Get hash	malicious	Browse	• 37.123.118.150
	XKLyPH8fil.exe	Get hash	malicious	Browse	• 37.123.118.150
	Citation-HEQ211025001T-EXPP v4.pdf.exe	Get hash	malicious	Browse	• 37.123.118.150
	VSL_MV SEA-BLUE SHIP OWNERS.exe	Get hash	malicious	Browse	• 37.123.118.150
	Order.exe	Get hash	malicious	Browse	• 37.123.118.150
	New Offer.exe	Get hash	malicious	Browse	• 37.123.118.150
	202111161629639000582.exe	Get hash	malicious	Browse	• 37.123.118.150
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• 37.123.118.150

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\app	
Process:	C:\Users\user\Desktop\dxEOMYaOtV.exe
File Type:	UTF-8 Unicode (with BOM) text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	C6BDBC9D86009CCF7E8DE878C9603213
SHA1:	2A4B8716F978F2D107BCD8294B486A5EE45AFE6E
SHA-256:	36A067FDFCEE95EB270F0B72E3B9E40D52C907D749FB9A8490D82F8EE56B29EB
SHA-512:	C42A52CD8837E2533B3D5EC97639F0C94287E3D7A6C73635C21DF50EBA8483B60DF15BF262A308836875CD9AFED504E7F98A2F6B254E4181FE548B1853D4225
Malicious:	false
Reputation:	low
Preview:	.5

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	313
Entropy (8bit):	4.971939296804078
Encrypted:	false
SSDEEP:	6:/ojfKsUTGN8Ypox42k9L+DbGMKeQE+vigqAZs2E+AYeDPO+Yswyha:wjPIGNrkHk9iaeIM6ADDPOHyha
MD5:	689E2126A85BF55121488295EE068FA1
SHA1:	09BAAA253A49D80C18326DFBCA106551EBF22DD6
SHA-256:	D968A966EF474068E41256321F77807A042F1965744633D37A203A705662EC25
SHA-512:	C3736A8FC7E6573FA1B26FE6A901C05EE85C55A4A276F8F569D9EADC9A58BEC507D1BB90DBF9EA62AE79A6783178C69304187D6B90441D82E46F5F56172B5C5C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..IMPORTANT: Command executed successfully...However, "netsh firewall" is deprecated;..use "netsh advfirewall firewall" instead...For more information on using "netsh advfirewall firewall" commands..instead of "netsh firewall", see KB article 947709..at https://go.microsoft.com/fwlink/?linkid=121488 .....Ok.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.567952442278428
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	dxEOMYaOtV.exe
File size:	95232
MD5:	a20a44e2add8f2ee2434258a20ac815e
SHA1:	bf2886c5bda80c2cc1a1a8d3d270f3e82f3f39b9
SHA256:	87b9a82fa05019692e89dc944a4fe1ab669d1c844abfd509c7e3648a024d4a73
SHA512:	ebb8b81d74aaf9475f64a23116da3d62497a6c92f6a7ac33fdcb7895e0aab6419c86ab92e104dc66cfc13a5bd0faa104fb3a997ce7bcfd0044e2ad3d25273e36

General

SSDEEP:	1536:RUXTr1IDavlZhbSKa9YdjEwzGi1dDyD6gS:RUXSDavlZIXmqi1dk/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.a.....p..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x418f2e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A921A0 [Thu Dec 2 19:42:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x16f34	0x17000	False	0.368089758832	data	5.59964154951	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x1a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: dxEOMYaOtV.exe PID: 7008 Parent PID: 5528

General

Start time:	00:30:18
Start date:	05/12/2021
Path:	C:\Users\user\Desktop\dxEOMYaOtV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dxEOMYaOtV.exe"
Imagebase:	0x3b0000
File size:	95232 bytes
MD5 hash:	A20A44E2ADD8F2EE2434258A20AC815E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.1182843286.00000000003B2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.1182843286.00000000003B2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000000.656185698.00000000003B2000.00000002.00020000.sdmp, Author: Joe Security • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000000.656185698.00000000003B2000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.1183435675.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: netsh.exe PID: 7096 Parent PID: 7008

General

Start time:	00:30:20
Start date:	05/12/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram "C:\Users\user\Desktop\dxEOMYaOtV.exe" "dxEOMYaOtV.exe" ENABLE
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7108 Parent PID: 7096

General

Start time:	00:30:21
Start date:	05/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis