ID: 553010
Sample Name: 3NeufRwoxF
Cookbook: default.jbs
Time: 04:15:16
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

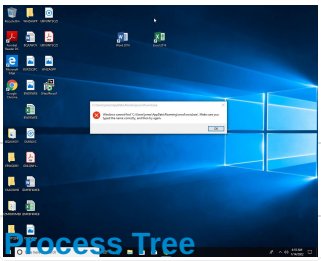
Windows Analysis Report 3NeufRwoxF

Overview

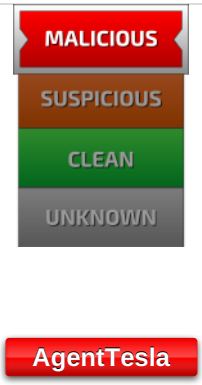
General Information

Sample Name:	3NeufRwoxF (renamed file extension from none to exe)
Analysis ID:	553010
MD5:	891fafcb65f039c…
SHA1:	e9ca83ec5e9a92..
SHA256:	3c6d3aa382ddba..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



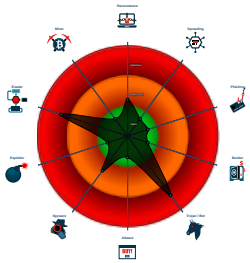
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Multi AV Scanner detection for dropp…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Queries sensitive BIOS Information …
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…

Classification



- **System is w10x64**
- 3NeufRwoxF.exe (PID: 4484 cmdline: "C:\Users\user\Desktop\3NeufRwoxF.exe" MD5: 891FAFCB65F039CEFAC6701BFB8A9253)
  - 3NeufRwoxF.exe (PID: 4828 cmdline: "C:\Users\user\Desktop\3NeufRwoxF.exe" MD5: 891FAFCB65F039CEFAC6701BFB8A9253)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info.superseal@yandex.com",
  "Password": "Golddigger",
  "Host": "smtp.yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000001.655268530.000000000400000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000001.655268530.000000000400000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000000.654698567.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.654698567.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000003.730336959.000000000824000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.3NeufRwoxF.exe.415058.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.3NeufRwoxF.exe.415058.7.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.3NeufRwoxF.exe.23c0000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.3NeufRwoxF.exe.23c0000.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.3NeufRwoxF.exe.23c0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 51 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

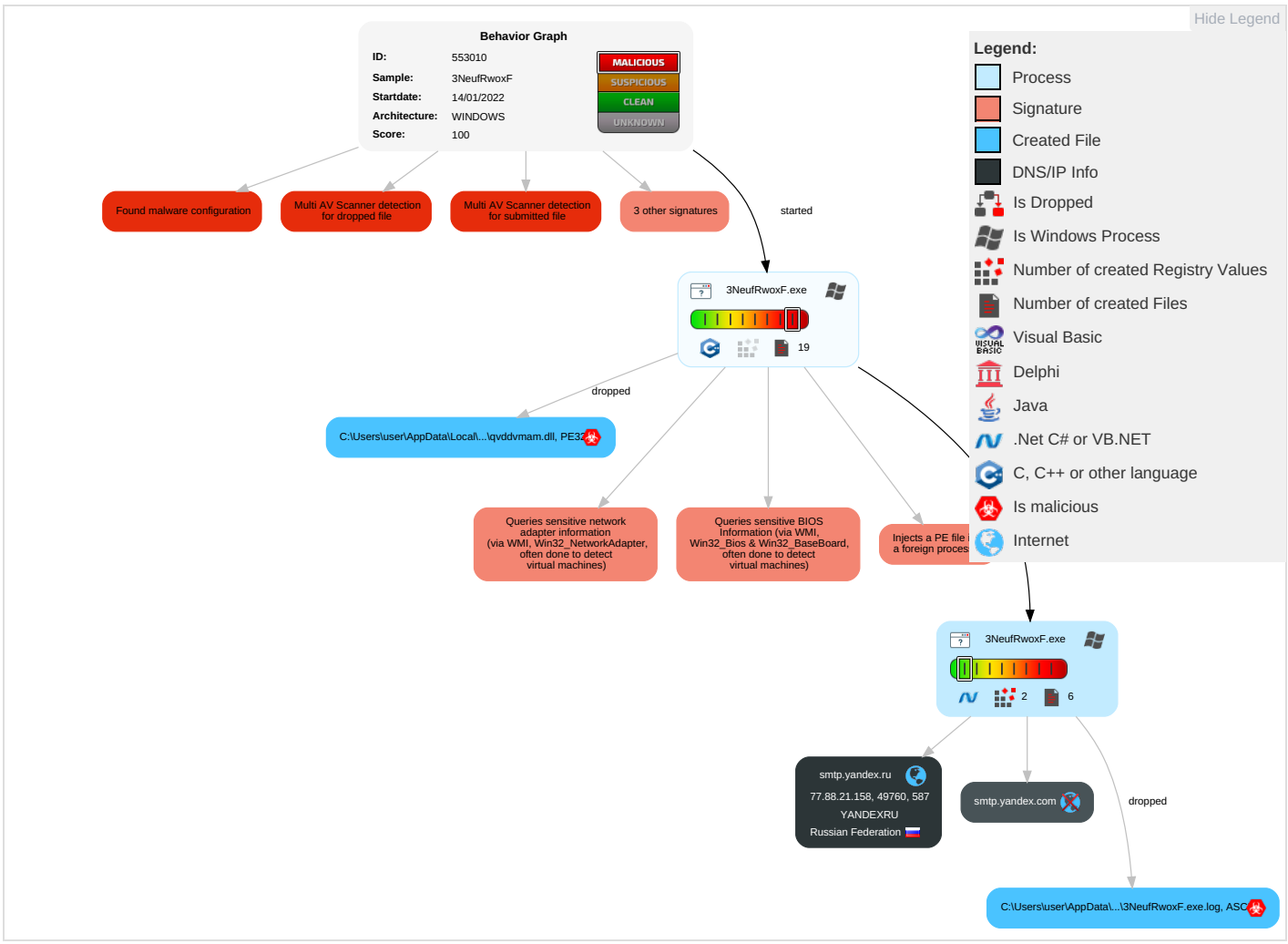
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	En Ch
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Nc Po
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Nc Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 1 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Security Software Discovery 2 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Virtualization/Sandbox Evasion 1 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
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	Fil Pr

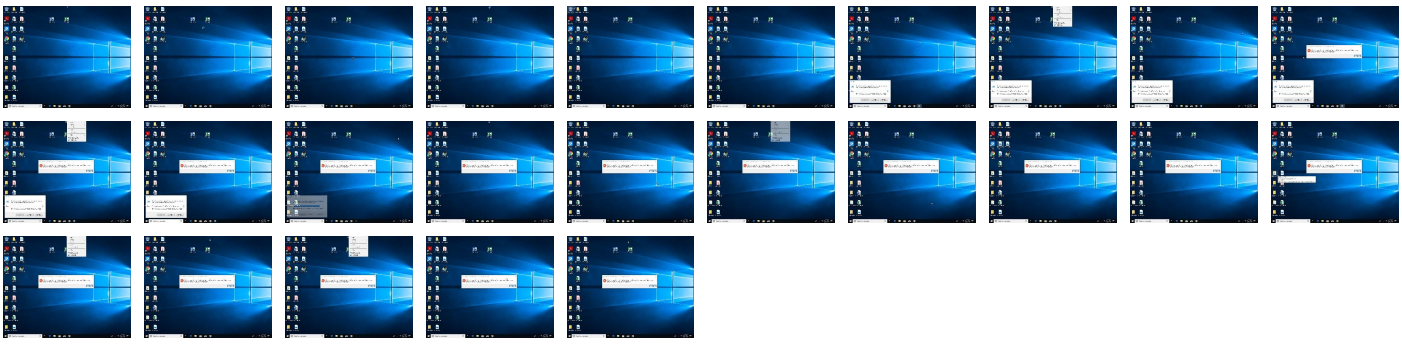
Behavior Graph

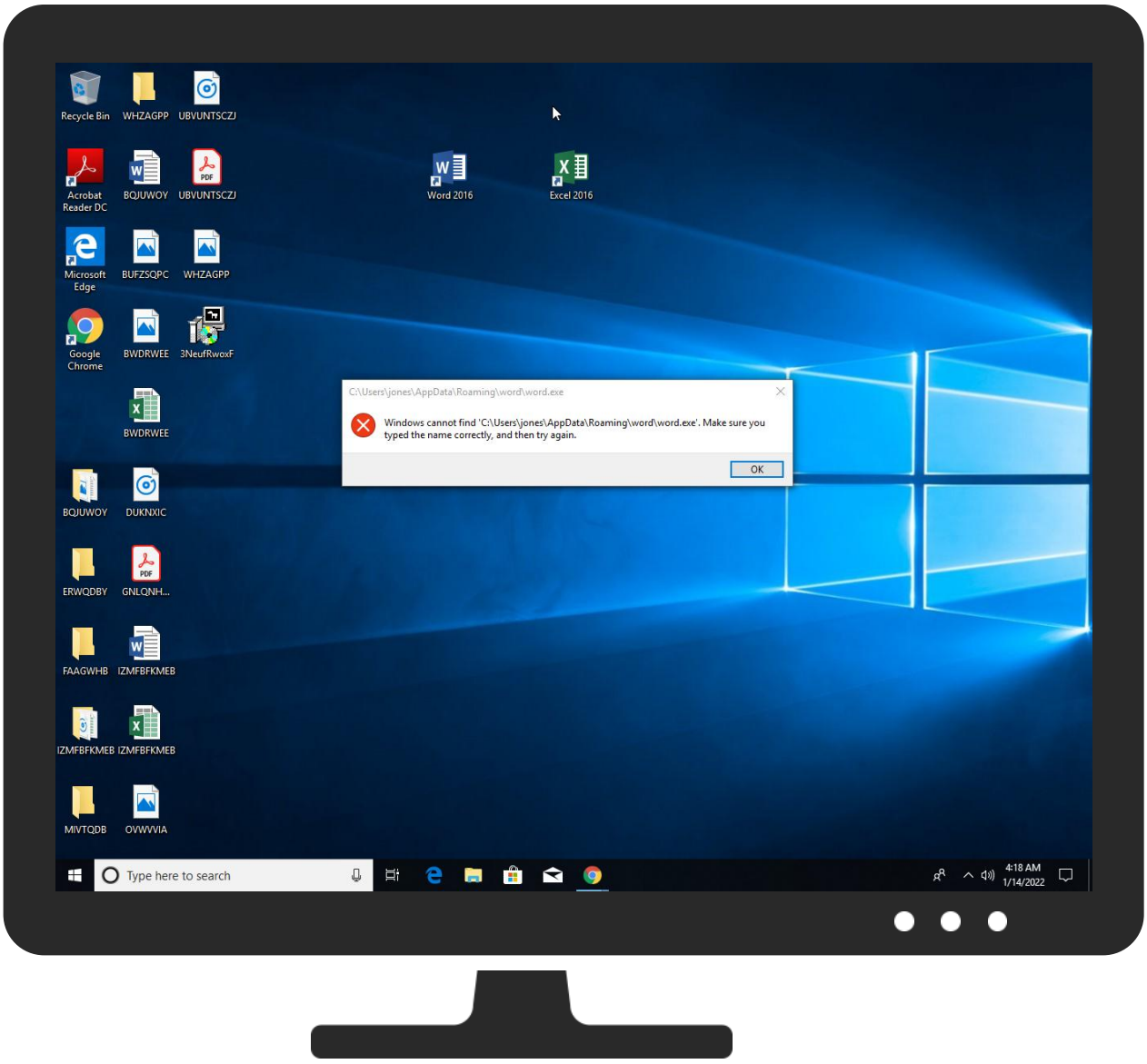


Screenshots

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
3NeufRwoxF.exe	45%	Virustotal		Browse
3NeufRwoxF.exe	51%	ReversingLabs	Win32.Trojan.AgentTesla	
3NeufRwoxF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsvCA57.tmp\qvddvmam.dll	43%	ReversingLabs	Win32.Trojan.SpyNoon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.3NeufRwoxF.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.3NeufRwoxF.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.3NeufRwoxF.exe.49d0000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.3NeufRwoxF.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.3NeufRwoxF.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.3NeufRwoxF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.3NeufRwoxF.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.3NeufRwoxF.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.3NeufRwoxF.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.3NeufRwoxF.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com0.	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://yandex.oc	0%	Avira URL Cloud	safe	
http://crls.ya	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://MXCHOJ.com	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://yandex.ocsp-responder.com03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553010
Start date:	14.01.2022
Start time:	04:15:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3NeufRwoxF (renamed file extension from none to 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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/5@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 55.1% (good quality ratio 50.9%) • Quality average: 77.6% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
04:16:14	API Interceptor	228x Sleep call for process: 3NeufRwoxF.exe modified
04:16:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run word C:\Users\user\AppData\Roaming\word\word.exe
04:16:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run word C:\Users\user\AppData\Roaming\word\word.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\3NeufRwoxF.exe.log

Process:	C:\Users\user\Desktop\3NeufRwoxF.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\3NeufRwoxF.exe.log	
Category:	dropped
Size (bytes):	1035
Entropy (8bit):	5.26629226223271
Encrypted:	false
SSDEEP:	24:MLF20NaL329hJ5g522rWz2pmyE49EY829XBp26K95rKoO2+g2+:MwLLG9h3go2rG2Iyb9P9XBY6ox+g2+
MD5:	B1B758A3B5F51F96241EF50244ADD244
SHA1:	FA513B977BF2DF5B6F279046B2D7B4BA024D3B68
SHA-256:	BAAFDBA30F16DFCDBC5601E4166BD5E1D3A1EAA08E9E68E44A96B00206222481
SHA-512:	A683EEEF8F41FE80EC1EFD262CE023951B262ADD965F7A0610D6A92B6C1B561D3F6ECBF165122DB06DD085D5FC19956C047C18D7CA012E549D7DE48BB0E0C18
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\CustomMarshalers\6e9bdd78f7a8bb20d228fefdaa957d00\CustomMarshalers.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261edb63c93616550f034\System.Management.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d

C:\Users\user\AppData\Local\Temp\kusazc8wp39	
Process:	C:\Users\user\Desktop\3NeufRwoxF.exe
File Type:	data
Category:	dropped
Size (bytes):	292351
Entropy (8bit):	7.963680613819231
Encrypted:	false
SSDEEP:	6144:5J7j/PKBR0SZfeudE96KIb/78b99INzXBtVpffaPS6GXBapeYv3kXteyg:DP+HZW196KIzjNzXBLpXRFAAYvIFg
MD5:	B5CCA07383DB50DF2C8791E4D49D0388
SHA1:	A0C0F92616231ECC57C819E52F672CF31360A7D8
SHA-256:	52C89193D7D69F546AC45181644669C0FBB7F71BC892361043E7D197007A3332
SHA-512:	19B0A0CC4C4066B543F574B22A1B5078F0691B77C32F9395AC11D42720A9A2BB05B119F6983280567E234AF15F5E6A3C6C57FC4EEEA0B7AE9EFF730310C5259B
Malicious:	false
Reputation:	low
Preview:	.|m...Y.u.....#I.g.T2~J.-n0....?..c..;.....oR....O.|D.U5.....o..Zu...Z.....^z.s{...9(...+H.....:skY..c./.Q)..S...3K..'\.....6..Aw...Oy..D...C..4.....,G.H[..... .....l..L....X...(.|u..\.....".*.[,..|...m...n....2Y..pE.....G.+...k....Y..i....#cT&sT2~J.-n0..L.(.c..;.....oR.^..OQ|D.l5..5...r...{...~.....j5.....@...o$.2..>.z..'s.77J..H.~H.....K..)K..Zr..vT.....+.e..#J.f..C.1....!...i).$P..K&..o!...^/<.....=,I.]..gT:v.....t..A.'....,.....H.....#...G.+.....1L1.Y.6...a,.#..g.T%~J.-n0....?..c..;;.N..ooR!u..O.|D..5.....e~..G...z.i...;DQ...5.2`...$E..&'s'77J.9H^.H.v*.*.-..mK..([.U.t.a...+....2.f..Cm1...}...i).....v.k../<.....=,I....dT:v.....j...t..A.'.....H.....#...G.+...k....Y.....aN.#..g.T2~J.-n0....?..c..;.....oR....O.\|D.U5..5.....e~.....5.....WQ...$.2.....&'s'77J.9H..H.....3K..)K..Zr.U.t.a...+....2.f..C.1....!...i).$P..K&.{..k.^/<.....=,I.]..gT:v.....j...t..A.'.....

C:\Users\user\AppData\Local\Temp\nsvCA56.tmp	
Process:	C:\Users\user\Desktop\3NeufRwoxF.exe
File Type:	data
Category:	dropped
Size (bytes):	329718
Entropy (8bit):	7.759225914420623
Encrypted:	false
SSDEEP:	6144:W0J7j/PKBR0SZfeudE96KIb/78b99INzXBtVpffaPS6GXBapeYv3kXteyDX:ZP+HZW196KIzjNzXBLpXRFAAYvIFD
MD5:	450A7BE54EEBE6430CCF5B72345E6BF8
SHA1:	E671D233C186B44CC64C9FBAF6A3A6846CF7A5D9
SHA-256:	6326557B1B47C65C963867B910E628D4DF7685307BAA31A106EF6180D817174D
SHA-512:	2234CB5484ED783FD5955BAA6811345EB9A8C4A976B80697487A277F3D2002F39DC3C92A399807E8537F97E1CD7EC593E6845E4E02D82052B4FC95BA3837B958
Malicious:	false
Reputation:	low
Preview:	wk.....,.....s....R.....j.....k..... .....J.....j.....~..... ....

C:\Users\user\AppData\Local\Temp\nsvCA57.tmp\qvddvmam.dll	
Process:	C:\Users\user\Desktop\3NeufRwoxF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.76274363382061
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsvCA57.tmp\qvddvmam.dll	
SSDEEP:	24:e31GSNND0teIASdax/++mMTJK4f9Y/2rY/noNXs+f3SlLRQ0K7ABPnRuV4MPgicT:Cn4I90IKyzJFbfGFN1RuqSm
MD5:	E7CB1AB1779B1AACEDD03A0E490E0318
SHA1:	9085E849395D59F1EFA1038484A0D99355CFEF51
SHA-256:	0668DF84EEDD97C9003610F70F2C9BE76605C40A6452B6B8A739C1BC102330EF
SHA-512:	2B482173601C59EB691D230934CACA8C716E07FA18BC8EA388CC8A3B98004C5A5EFADED903E5F3817D9084319ABCBCADF51C698E2D5C254BE0A034044F4FFE85
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 43%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z-...C]..C]..C]Z.M]..C].}B\..C]..B]..C].nG\..C].nC\..C].n.]..C].nA\..C]Rich..C].....PE..L.....a.....!..... .....P.....@..... ..L.... .....0.....@..<.....text.../..... ..`.rdata..... .....@..@.rsrc.....0.....@..@.reloc..<....@.....@..B.....

C:\Users\user\AppData\Local\Temp\wuatpe	
Process:	C:\Users\user\Desktop\3NeufRwoxF.exe
File Type:	data
Category:	dropped
Size (bytes):	5232
Entropy (8bit):	6.1063109867064895
Encrypted:	false
SSDEEP:	96:2wMTU6r2dfPoqv106Yo2QdQ0xsCqtAE3Lm7eW03d3AKfxWTaAIHq:XMTTr2dIqv106hv0tAYmqA4xWhIHq
MD5:	29323A6559E425DA23E2AEA82AB47558
SHA1:	C8A00930296EE9259ED13A8AE96DC019C402891E
SHA-256:	0295E73A190C03EF64A394D02E8DB03ADACD8D6EBA54131975204CDEAF88D59E
SHA-512:	B127F9D563830CD0F11AABC1E20CB906EE9AC16B83BE276162FF1C9F2A002169051630D65ABC06B8750F763A63AF1840C7DDBF30A72967FB2F5E2671FC04E53
Malicious:	false
Reputation:	low
Preview:	.....{.H...{...W..WKE(W..WKE {....E.`...{....uT.uX.E. .....E..$.uT.uX.E. ....E....uT.uX.E. .....E....uT.uX.E. .....E...{mX.nBr..s...ET..E(...EX{ .+..E .}..E .}....+.rX....E .....E.....{..r+....{.\..3...u...u...u.A..u.A..u(..u ...lX.@.T.@..h{..u..u.A..E.W..E.... .....<\.[...{.\=....E.....%..T.....W..WKE..E...CETkh.E....}X.L....<...E..E...H.}....E....%..T..N... p... v....L....'. ....=.. ....{.`W..WKE .E.X....E..E.{m..lN.E.....E.H.E..E.@.E... L.....l>.E..r..s...<=..=$.E .r...!..<=..=$r.r..s...<.....'. ..... .....E..W.E ..u. .....E.{m..l.{.....E.....E..%.....{.HW..WKE .E.`....E..E.{m..lN.E.....E.H.E..E.@.E... ......W|.....E..r..s...<=..=..ET.r...!..<=..=..EX.r...!.<=..=..EL+.r..s...<U..U..E .r...!..<=..=.r.r..s...<...N... ....E.{mP.l..E .}P...O .uP.uL.uX.uT.u. /....E.{m..l.{.....E.....E..%..L....{.d.E.X....E..E.{m..lN.E.....E.H.E..E.@.E... r.....l>.E..r..s...<=..= .ET.r...!..<=..= r.r..s...<....=.. _.... \....E..V.u

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.937250521287509
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	3NeufRwoxF.exe
File size:	271670
MD5:	891fafcb65f039cefac6701bfb8a9253
SHA1:	e9ca83ec5e9a9264d251a3379d65dd9dfe92a16a
SHA256:	3c6d3aa382ddba97862136aa06c449150810696ef7cb05e7ec0f4ed6895683c4
SHA512:	5e7ca6e15580aac04bfcafad2ab3bd681b4fd8808775b4353d543d666231bd85827ea6285eda0046eb661cf5d0609c25c6c247440eef2d26a4952851e16d1a11
SSDEEP:	6144:owLFeIPg68CqO4M+7UwS7nC3/WfB5cUnJ3nkr9/:f5Pg69znM3SjcUJ3nkrR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$../.{...$...%..:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 04:16:39.710926056 CET	192.168.2.4	8.8.8.8	0xe7fd	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 04:15:58.456048965 CET	8.8.8.8	192.168.2.4	0x6035	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 04:16:39.729899883 CET	8.8.8.8	192.168.2.4	0xe7fd	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 04:16:39.729899883 CET	8.8.8.8	192.168.2.4	0xe7fd	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 04:16:40.092539072 CET	587	49760	77.88.21.158	192.168.2.4	220 vla5-8422ddc3185d.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1642130200-NCDFImhoWk-GdQSG1m3
Jan 14, 2022 04:16:40.092818022 CET	49760	587	192.168.2.4	77.88.21.158	EHLO 305090
Jan 14, 2022 04:16:40.148118019 CET	587	49760	77.88.21.158	192.168.2.4	250-vla5-8422ddc3185d.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 14, 2022 04:16:40.148405075 CET	49760	587	192.168.2.4	77.88.21.158	STARTTLS
Jan 14, 2022 04:16:40.203632116 CET	587	49760	77.88.21.158	192.168.2.4	220 Go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 3NeufRwoxF.exe PID: 4484 Parent PID: 6372

General

Start time:	04:16:03
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\3NeufRwoxF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3NeufRwoxF.exe"
Imagebase:	0x400000
File size:	271670 bytes
MD5 hash:	891FAFCB65F039CEFAC6701BFB8A9253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.656663064.0000000003020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.656663064.0000000003020000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 3NeufRwoxF.exe PID: 4828 Parent PID: 4484

General

Start time:	04:16:04
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\3NeufRwoxF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3NeufRwoxF.exe"
Imagebase:	0x400000
File size:	271670 bytes
MD5 hash:	891FAFCB65F039CEFAC6701BFB8A9253
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.655268530.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000001.655268530.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.654698567.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.654698567.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000003.730336959.0000000000824000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000003.730336959.0000000000824000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.653816558.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.653816558.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.734722737.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.734722737.00000000038D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.734429027.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.734429027.00000000028D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.734344539.00000000023C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.734344539.00000000023C0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.734912309.00000000049D2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.734912309.00000000049D2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.733760702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.733760702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Disassembly

Code Analysis