ID: 451394
Sample Name:
nZdwtTEYoW.exe
Cookbook: default.jbs
Time: 15:58:22
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

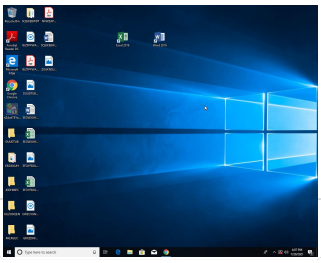
Windows Analysis Report nZdwtTEYoW.exe

Overview

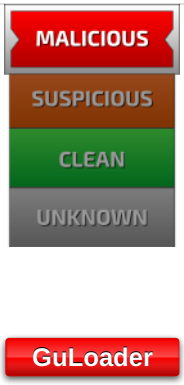
General Information

Sample Name:	nZdwtTEYoW.exe
Analysis ID:	451394
MD5:	c8feb9d53b567cd..
SHA1:	82a22cb59d46ba..
SHA256:	642a0df15a9b8e3.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



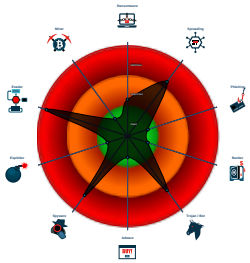
GuLoader

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

Signatures

- GuLoader behavior detected
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Detected RDTSC dummy instruction…
- Found evasive API chain (trying to d…
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- nZdwtTEYoW.exe (PID: 6052 cmdline: 'C:\Users\user\Desktop\nZdwtTEYoW.exe' MD5: C8FEB9D53B567CD1BFB0E59CF7D26BC2)
  - RegAsm.exe (PID: 4180 cmdline: 'C:\Users\user\Desktop\nZdwtTEYoW.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 4816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

Networking:

Sigma detected: RegAsm connects to smtp port

Jbx Signature Overview

Click to jump to signature section

Copyright Joe Security LLC 2021

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

GuLoader behavior detected

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

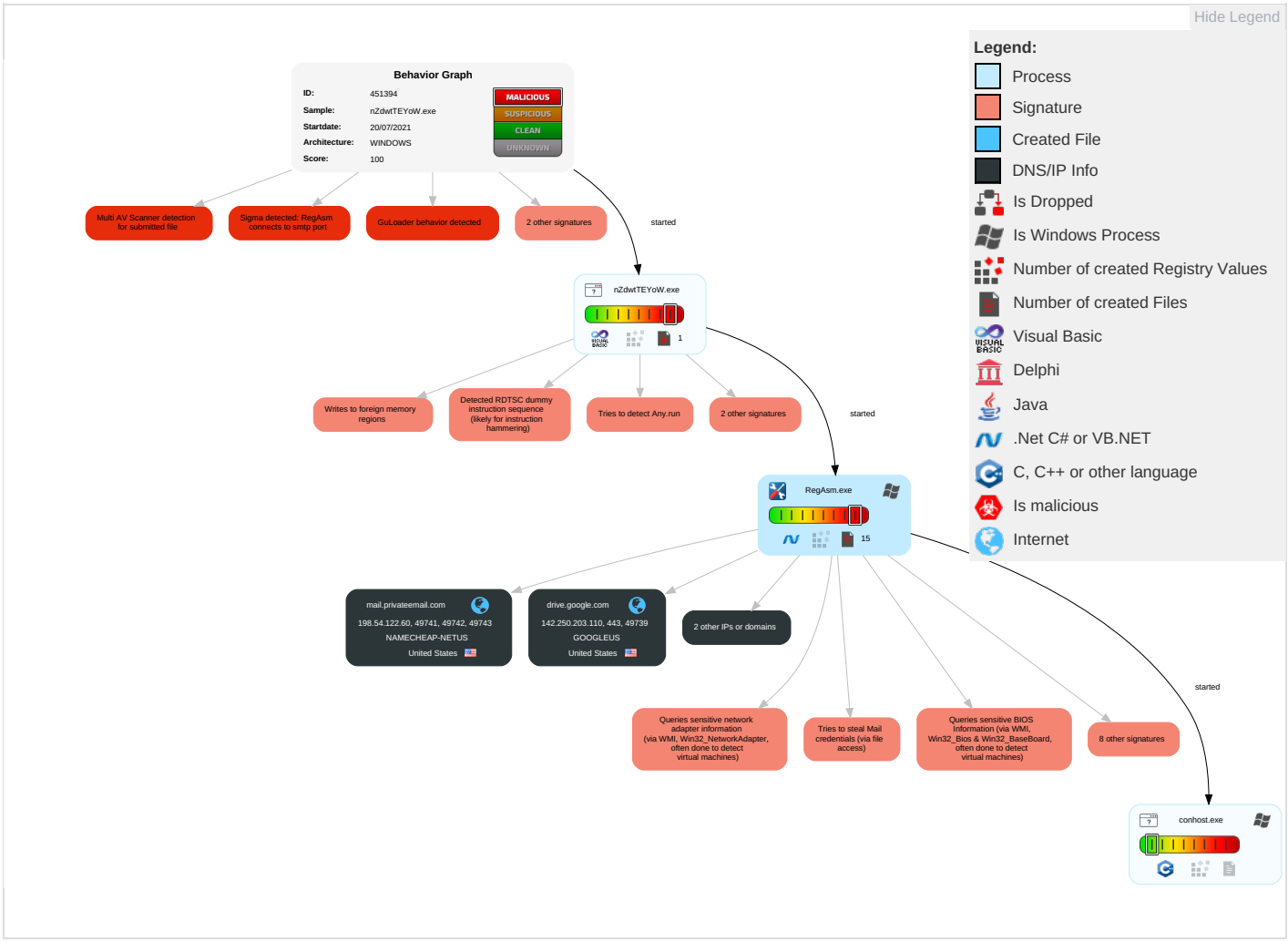
Tries to steal Mail credentials (via file access)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 6 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 1 1 1	Process Discovery 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 4 1	Security Account Manager	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Appli Layer Proto

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 3 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used

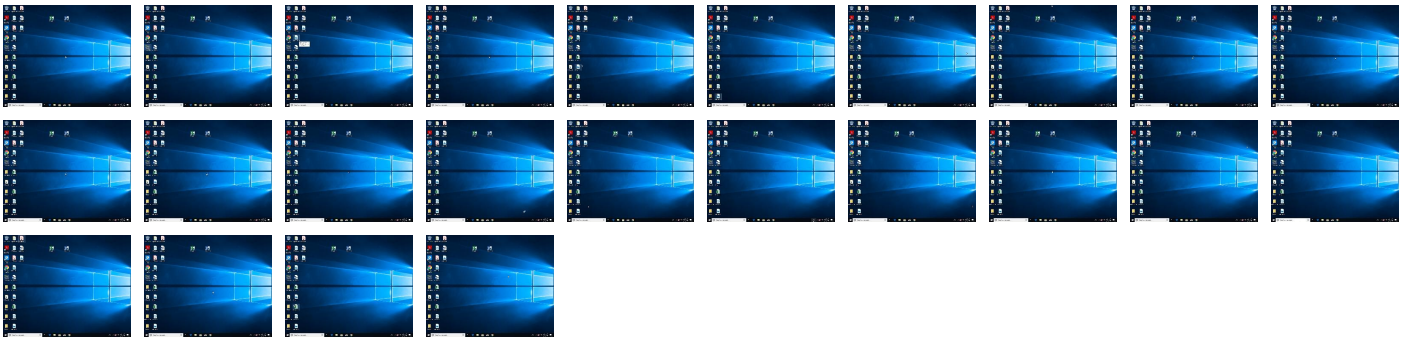
Behavior Graph



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
nZdwtTEYoW.exe	25%	Virustotal		Browse
nZdwtTEYoW.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	
nZdwtTEYoW.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ocsp.sectigo.	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	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://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://sectigo.com/C	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high
drive.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
doc-0k-ak-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.203.110	drive.google.com	United States		15169	GOOGLEUS	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451394
Start date:	20.07.2021
Start time:	15:58:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nZdwtTEYoW.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	44
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.spyw.evad.winEXE@4/2@25/3
EGA Information:	Failed
HDC Information:	Failed
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
16:01:24	API Interceptor	1648x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	
	Shipping Documents .doc	Get hash	malicious	Browse	
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	
	Inv PKF312021.doc	Get hash	malicious	Browse	
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	20210716001.exe	Get hash	malicious	Browse	
	20210716001.exe	Get hash	malicious	Browse	
	Inquiry-Order.exe	Get hash	malicious	Browse	
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	
	JaqsKbRJ8w.exe	Get hash	malicious	Browse	
	neGJUsBCPT.exe	Get hash	malicious	Browse	
	5Q2N9nbIIR.exe	Get hash	malicious	Browse	
	BOQ.doc	Get hash	malicious	Browse	
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	
	9PcMMlkF9y.exe	Get hash	malicious	Browse	
	6mBVAJrIcy.exe	Get hash	malicious	Browse	
	TpLxV14aT3.exe	Get hash	malicious	Browse	
	requirement010.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.privateemail.com	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 198.54.122.60
	Shipping Documents .doc	Get hash	malicious	Browse	• 198.54.122.60
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 198.54.122.60
	Inv PKF312021.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 198.54.122.60
	SOA.exe	Get hash	malicious	Browse	• 198.54.122.60
	20210716001.exe	Get hash	malicious	Browse	• 198.54.122.60
	20210716001.exe	Get hash	malicious	Browse	• 198.54.122.60
	Inquiry-Order.exe	Get hash	malicious	Browse	• 198.54.122.60
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	• 198.54.122.60
	JaqsKbRJ8w.exe	Get hash	malicious	Browse	• 198.54.122.60
	neGJUsBCPT.exe	Get hash	malicious	Browse	• 198.54.122.60
	5Q2N9nbIIR.exe	Get hash	malicious	Browse	• 198.54.122.60
	BOQ.doc	Get hash	malicious	Browse	• 198.54.122.60
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	• 198.54.122.60
	9PcMMlkF9y.exe	Get hash	malicious	Browse	• 198.54.122.60
	6mBVAJrIcy.exe	Get hash	malicious	Browse	• 198.54.122.60
	TpLxV14aT3.exe	Get hash	malicious	Browse	• 198.54.122.60
	requirement010.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 198.54.122.60
	Shipping Documents .doc	Get hash	malicious	Browse	• 198.54.122.60
	QxnlprRUTx.exe	Get hash	malicious	Browse	• 199.188.200.230
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 198.54.122.60
	Statement.xlsx	Get hash	malicious	Browse	• 162.0.237.9
	Inv PKF312021.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 198.54.122.60
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	Order.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 198.54.122.60
	Inv_7623980.exe	Get hash	malicious	Browse	• 63.250.34.223
	xBMx9OBP97.exe	Get hash	malicious	Browse	• 198.54.114.131
	CSyG3zNcwS.exe	Get hash	malicious	Browse	• 198.54.114.131
	BrCi5pJr8J.exe	Get hash	malicious	Browse	• 198.54.114.131
	QQ9XxgbU1G.exe	Get hash	malicious	Browse	• 198.54.114.131
	20210716001.exe	Get hash	malicious	Browse	• 198.54.122.60
	WR0MTpWkYC.exe	Get hash	malicious	Browse	• 198.54.114.131

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LPY15536W4.exe	Get hash	malicious	Browse	• 198.54.117.211
	frank.connardiii@globalfoundries.com_34834865Application.HTM	Get hash	malicious	Browse	• 68.65.122.97

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	unJLhL75HG.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	9bCnBwR693.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	BVD1xWp0y0.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	nRjbMQ5Jua.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Hsbc Scan copy 3547856788 Pdf.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	DigitalLicense.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	vir.dll	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	#Ud53c#Uc544#Ub178.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	INV #95000987.html	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	F63V4i8eZU.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Doc_PDF.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	5S6Cod7HCf.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	SecuriteInfo.com.W32.AIDetect.malware2.14010.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	xy3zf2YjS8.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	2dgOIcIVVb.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	2m4OlrMaLT.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	WOVngDEXHM.dll	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	VUBuRErqKh.dll	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97

Dropped Files

No context

Copyright Joe Security LLC 2021

Created / dropped Files

C:\Users\user\AppData\Roaming\1t4tqdc1.agl\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.4666127843418355
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	nZdwtTEYoW.exe
File size:	118784
MD5:	c8feb9d53b567cd1bfb0e59cf7d26bc2
SHA1:	82a22cb59d46bae21fa4877015e163eacc04a022
SHA256:	642a0df15a9b8e3124d638e755f0bdbacd0d1c3ff01b59b36213a190a5e5645a
SHA512:	da707134a7bfdcb66389f111bb363d1e7b7260bb718d6ae999a23fc538e2065d8be766a713d8d20860e835eb21609bbbcb0d0b6c237124fa38bd2ada04acf157
SSDEEP:	1536:/bjX1R6rHR+Gz6YsFdVfKcLe0NMDfuoFVHYGokXYtvcOOfgrJZ+R6rHJXdb:jjX1yH1HErzwmoFtoZtkJgrCyHJXd

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....!.Q.....@.....(.....P....@.....

File Icon

Icon Hash:	b29a4a4a5a4a4a45

Static PE Info

General

Entrypoint:	0x401128
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:	0x510121E6 [Thu Jan 24 11:58:30 2013 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:	5c4d602843f54570889588b32f7af650

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13d90	0x14000	False	0.640209960938	data	6.90665747983	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x6d6a	0x7000	False	0.566301618304	data	5.78429982153	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Maltese	Malta	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 16:01:16.561033010 CEST	192.168.2.3	8.8.8.8	0x5431	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:17.522702932 CEST	192.168.2.3	8.8.8.8	0x9b80	Standard query (0)	doc-0k-ak-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:49.130983114 CEST	192.168.2.3	8.8.8.8	0x72a6	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:53.596967936 CEST	192.168.2.3	8.8.8.8	0x807c	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:58.489578962 CEST	192.168.2.3	8.8.8.8	0x9b5e	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:03.642308950 CEST	192.168.2.3	8.8.8.8	0xa7be	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:09.503528118 CEST	192.168.2.3	8.8.8.8	0xb30d	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:16.476000071 CEST	192.168.2.3	8.8.8.8	0x76ff	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:23.505131006 CEST	192.168.2.3	8.8.8.8	0x7c28	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:31.021351099 CEST	192.168.2.3	8.8.8.8	0xdbfe	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:38.307100058 CEST	192.168.2.3	8.8.8.8	0xf9e6	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:45.829462051 CEST	192.168.2.3	8.8.8.8	0xe75a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:52.933203936 CEST	192.168.2.3	8.8.8.8	0xf58b	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:53.723814011 CEST	192.168.2.3	8.8.8.8	0x3720	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:56.978291035 CEST	192.168.2.3	8.8.8.8	0xd4b	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:02.120524883 CEST	192.168.2.3	8.8.8.8	0xaaab	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:08.339550018 CEST	192.168.2.3	8.8.8.8	0xf053	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:14.666552067 CEST	192.168.2.3	8.8.8.8	0xc9cf	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:21.407037020 CEST	192.168.2.3	8.8.8.8	0x7fa9	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:27.999461889 CEST	192.168.2.3	8.8.8.8	0x4517	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:34.842991114 CEST	192.168.2.3	8.8.8.8	0xc4c0	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:41.899107933 CEST	192.168.2.3	8.8.8.8	0x8d83	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:48.829394102 CEST	192.168.2.3	8.8.8.8	0x1e6a	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:56.542314053 CEST	192.168.2.3	8.8.8.8	0xd7be	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Jul 20, 2021 16:04:12.056706905 CEST	192.168.2.3	8.8.8.8	0x7218	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 16:01:16.629291058 CEST	8.8.8.8	192.168.2.3	0x5431	No error (0)	drive.google.com		142.250.203.110	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 16:01:17.588656902 CEST	8.8.8.8	192.168.2.3	0x9b80	No error (0)	doc-0k-ak-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2021 16:01:17.588656902 CEST	8.8.8.8	192.168.2.3	0x9b80	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:49.187897921 CEST	8.8.8.8	192.168.2.3	0x72a6	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:53.655529976 CEST	8.8.8.8	192.168.2.3	0x807c	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:01:58.551398039 CEST	8.8.8.8	192.168.2.3	0x9b5e	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:03.702356100 CEST	8.8.8.8	192.168.2.3	0xa7be	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:09.563635111 CEST	8.8.8.8	192.168.2.3	0xb30d	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:16.528083086 CEST	8.8.8.8	192.168.2.3	0x76ff	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:23.561988115 CEST	8.8.8.8	192.168.2.3	0x7c28	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:31.073971033 CEST	8.8.8.8	192.168.2.3	0xdbfe	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:38.359966040 CEST	8.8.8.8	192.168.2.3	0xf9e6	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:45.881372929 CEST	8.8.8.8	192.168.2.3	0xe75a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:52.991389036 CEST	8.8.8.8	192.168.2.3	0xf58b	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:53.776395082 CEST	8.8.8.8	192.168.2.3	0x3720	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:02:57.038001060 CEST	8.8.8.8	192.168.2.3	0xd4b	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:02.177850962 CEST	8.8.8.8	192.168.2.3	0xaaab	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:08.399729013 CEST	8.8.8.8	192.168.2.3	0xf053	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:14.723648071 CEST	8.8.8.8	192.168.2.3	0xc9cf	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:21.468868017 CEST	8.8.8.8	192.168.2.3	0x7fa9	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:28.050875902 CEST	8.8.8.8	192.168.2.3	0x4517	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:34.899969101 CEST	8.8.8.8	192.168.2.3	0xc4c0	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:41.956672907 CEST	8.8.8.8	192.168.2.3	0x8d83	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:48.879498959 CEST	8.8.8.8	192.168.2.3	0x1e6a	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:03:56.600330114 CEST	8.8.8.8	192.168.2.3	0xd7be	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 20, 2021 16:04:04.260910988 CEST	8.8.8.8	192.168.2.3	0x50da	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 16:04:12.110840082 CEST	8.8.8.8	192.168.2.3	0x7218	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 20, 2021 16:01:16.813116074 CEST	142.250.203.110	443	192.168.2.3	49739	CN=*.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 28 03:38:45 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Sep 20 03:38:44 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Jul 20, 2021 16:01:17.708937883 CEST	142.250.203.97	443	192.168.2.3	49740	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Mon Jun 28 05:06:51 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Mon Sep 20 05:06:50 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 20, 2021 16:01:49.611522913 CEST	587	49741	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:01:54.055201054 CEST	587	49742	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:01:58.973331928 CEST	587	49743	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:04.098764896 CEST	587	49746	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:04.099298954 CEST	49746	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:04.294552088 CEST	587	49746	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:04.295017958 CEST	49746	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:04.489243031 CEST	587	49746	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:09.969183922 CEST	587	49753	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:09.969434023 CEST	49753	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:10.166465998 CEST	587	49753	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:10.166765928 CEST	49753	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:10.367321014 CEST	587	49753	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:16.923929930 CEST	587	49756	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:16.924472094 CEST	49756	587	192.168.2.3	198.54.122.60	EHLO 724536

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 20, 2021 16:02:17.118699074 CEST	587	49756	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:17.119184971 CEST	49756	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:17.313260078 CEST	587	49756	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:23.973472118 CEST	587	49757	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:23.974122047 CEST	49757	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:24.171462059 CEST	587	49757	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:24.171804905 CEST	49757	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:24.368725061 CEST	587	49757	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:31.469063997 CEST	587	49758	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:31.471573114 CEST	49758	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:31.666650057 CEST	587	49758	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:31.667433023 CEST	49758	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:31.863683939 CEST	587	49758	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:38.764539957 CEST	587	49759	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:38.765013933 CEST	49759	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:38.962157011 CEST	587	49759	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:38.962588072 CEST	49759	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:39.160888910 CEST	587	49759	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:46.282213926 CEST	587	49760	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:46.282908916 CEST	49760	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:46.477880001 CEST	587	49760	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:46.478698015 CEST	49760	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:02:46.672389984 CEST	587	49760	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:02:53.390088081 CEST	587	49761	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:54.190349102 CEST	587	49762	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:02:54.190762043 CEST	49762	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:02:54.385458946 CEST	587	49762	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:02:57.444710970 CEST	587	49763	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:02.580193996 CEST	587	49764	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 20, 2021 16:03:02.580537081 CEST	49764	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:03:02.778055906 CEST	587	49764	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:03:08.798110008 CEST	587	49765	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:08.798660040 CEST	49765	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:03:08.995985031 CEST	587	49765	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:03:15.129210949 CEST	587	49766	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:21.910490990 CEST	587	49767	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:28.458374023 CEST	587	49768	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:28.462193012 CEST	49768	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:03:28.661011934 CEST	587	49768	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:03:35.303242922 CEST	587	49769	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:35.303745985 CEST	49769	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:03:35.501075029 CEST	587	49769	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:03:42.350254059 CEST	587	49770	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:42.350675106 CEST	49770	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:03:42.544569016 CEST	587	49770	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:03:42.545100927 CEST	49770	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:03:42.739053965 CEST	587	49770	198.54.122.60	192.168.2.3	220 Ready to start TLS
Jul 20, 2021 16:03:49.279462099 CEST	587	49771	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:03:56.998744965 CEST	587	49772	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:04:12.507214069 CEST	587	49777	198.54.122.60	192.168.2.3	220 PrivateEmail.com prod Mail Node
Jul 20, 2021 16:04:12.508210897 CEST	49777	587	192.168.2.3	198.54.122.60	EHLO 724536
Jul 20, 2021 16:04:12.704148054 CEST	587	49777	198.54.122.60	192.168.2.3	250-mta-07.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 20, 2021 16:04:12.818646908 CEST	49777	587	192.168.2.3	198.54.122.60	STARTTLS
Jul 20, 2021 16:04:13.012594938 CEST	587	49777	198.54.122.60	192.168.2.3	220 Ready to start TLS

Copyright Joe Security LLC 2021

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: nZdwtTEYoW.exe PID: 6052 Parent PID: 5728

General

Start time:	15:59:17
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\nZdwtTEYoW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nZdwtTEYoW.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	C8FEB9D53B567CD1BFB0E59CF7D26BC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: RegAsm.exe PID: 4180 Parent PID: 6052

General

Start time:	16:00:14
Start date:	20/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nZdwtTEYoW.exe'
Imagebase:	0xc30000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Copyright Joe Security LLC 2021

File Read

Analysis Process: conhost.exe PID: 4816 Parent PID: 4180

General

Start time:	16:00:14
Start date:	20/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021