ID: 483922
Sample Name: TOP URGENT.exe
Cookbook: default.jbs
Time: 16:20:28
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

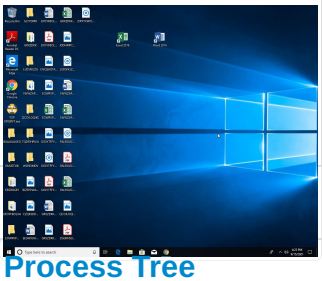
Windows Analysis Report TOP URGENT.exe

Overview

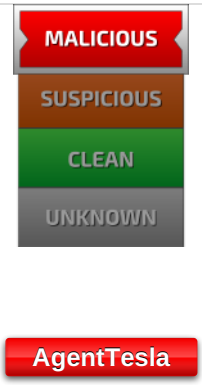
General Information

Sample Name:	TOP URGENT.exe
Analysis ID:	483922
MD5:	3af20ee616d2d9c.
SHA1:	f4448544d0fd560..
SHA256:	c810e257ac876c...
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



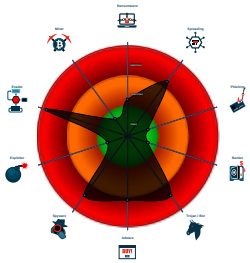
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: MSBuild connects ...
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi...
- Tries to harvest and steal ftp login c...
- Modifies the hosts file
- Tries to detect sandboxes and other...
- .NET source code contains potentia...

Classification



Process Tree

- **System is w10x64**
- TOP URGENT.exe (PID: 6352 cmdline: 'C:\Users\user\Desktop\TOP URGENT.exe' MD5: 3AF20EE616D2D9C806D27A3C245D4D7B)
  - MSBuild.exe (PID: 6592 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ppc@almuntakhaba.com",
  "Password": "amite123",
  "Host": "smtp.almuntakhaba.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.501627918.000000000298 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.501627918.000000000298 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.244947880.0000000002D9 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.245468332.0000000003D8 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.245468332.0000000003D8 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.TOP URGENT.exe.3e4d7b0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.TOP URGENT.exe.3e4d7b0.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.TOP URGENT.exe.3f5dfd0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

Networking:

Sigma detected: MSBuild connects to smtp port

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

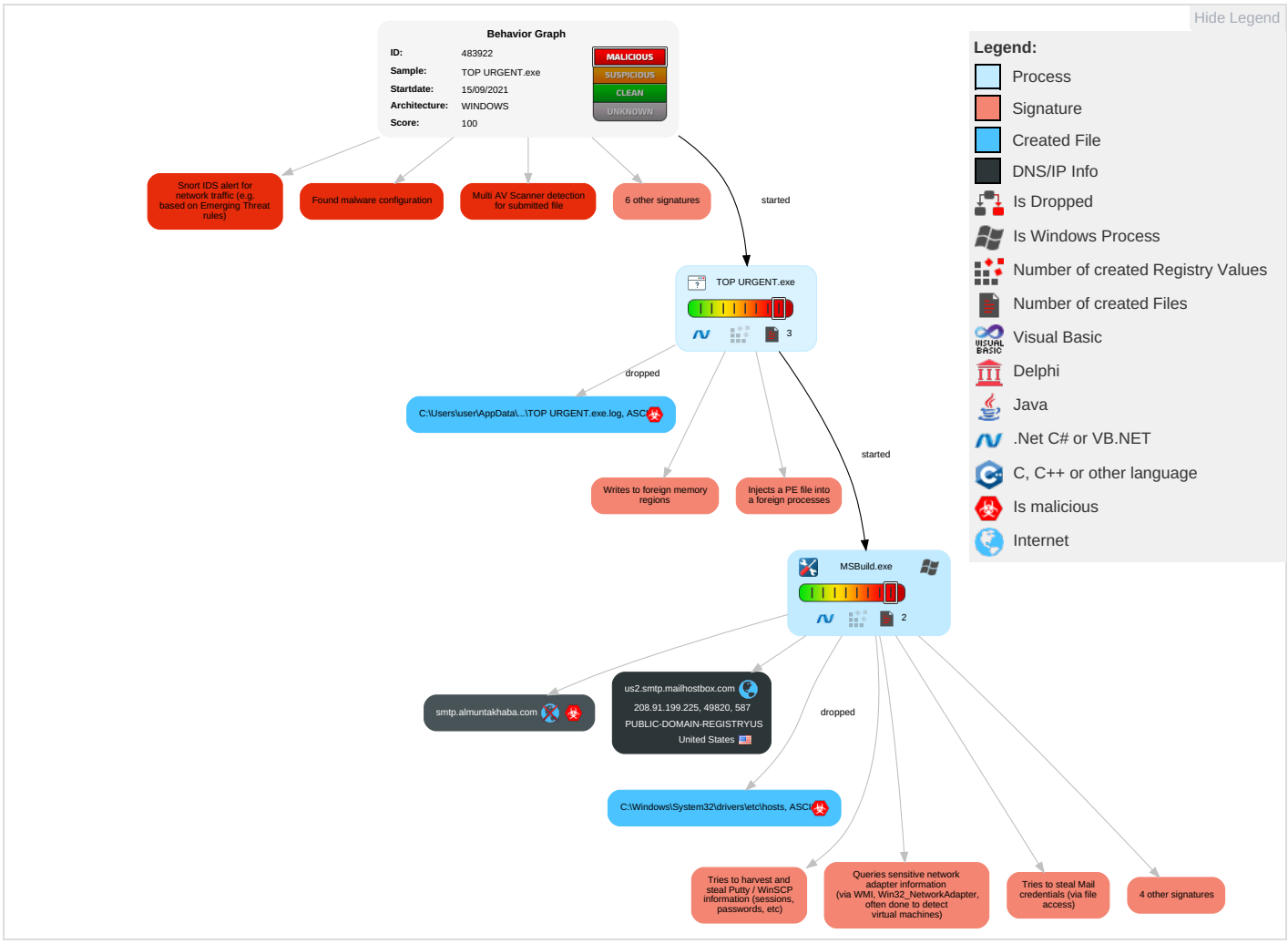
Remote Access Functionality:

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 2 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 2 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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
TOP URGENT.exe	16%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://smtp.almuntakhaba.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://bEdYOo.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://q77LAYiewN5yqbw.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high
smtp.almuntakhaba.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483922
Start date:	15.09.2021
Start time:	16:20:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TOP URGENT.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:	28
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.adwa.spyw.evad.winEXE@3/2@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:21:33	API Interceptor	1x Sleep call for process: TOP URGENT.exe modified
16:21:50	API Interceptor	675x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	HSBc20210216B1.exe	Get hash	malicious	Browse	
	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	
	RFQ#MAT#Quotation No. 20077253.exe	Get hash	malicious	Browse	
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	
	PaymentReceipt.doc	Get hash	malicious	Browse	
	Swift Transfer Copy mt103_PDF.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.MachineLearning.Anomalous.94.8891.exe	Get hash	malicious	Browse	
	PURCHASE ORDER 2021.exe	Get hash	malicious	Browse	
	L9d4ISc9LF4Yv1t.exe	Get hash	malicious	Browse	
	P.O_345.exe	Get hash	malicious	Browse	
	revised order-number 3A6.exe	Get hash	malicious	Browse	
	QUOTATION -PDF-SCAN-COPY.exe	Get hash	malicious	Browse	
	Urgent RFQ #2105031.pdf.exe	Get hash	malicious	Browse	
	Listed Items Order.exe	Get hash	malicious	Browse	
	order-2021-PO # 0834.xlsx	Get hash	malicious	Browse	
	qPlRnI13fW.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	VOn3J2hVHa.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	HSBc20210216B1.exe	Get hash	malicious	Browse	• 208.91.199.225
	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO- 45020032 Juv#U00e9l AS.exe	Get hash	malicious	Browse	• 208.91.199.224
	48q74tT5IK.exe	Get hash	malicious	Browse	• 208.91.199.224
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	• 208.91.199.225
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	• 208.91.199.224
	Final Sept Order #0921.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHL Express Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	ee5s192YZ34Ybve.exe	Get hash	malicious	Browse	• 208.91.199.223
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	• 208.91.199.224
	sapa list.doc	Get hash	malicious	Browse	• 208.91.198.143
	RFQ#MAT#Quotation No. 20077253.exe	Get hash	malicious	Browse	• 208.91.199.225
	04142021_10RD0207S0N0000,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	HY19071 PI.exe	Get hash	malicious	Browse	• 208.91.198.143
	PO_Contract_ANR07152112_20210715181907__110.exe	Get hash	malicious	Browse	• 208.91.198.143
	RFQ-#80986-3580.exe	Get hash	malicious	Browse	• 208.91.199.224
	Bank swift copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	i9fnXDoul7.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping Doc_968018592077_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB_968018592077_Invoice_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	HSBc20210216B1.exe	Get hash	malicious	Browse	• 208.91.199.225
	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO- 45020032 Juv#U00e9l AS.exe	Get hash	malicious	Browse	• 208.91.199.224
	Qoutation for Strips.doc	Get hash	malicious	Browse	• 162.215.24 1.145
	48q74tT5IK.exe	Get hash	malicious	Browse	• 208.91.199.224
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	• 208.91.199.225
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	• 208.91.199.224
	angelzx.exe	Get hash	malicious	Browse	• 162.215.24 1.145
	Final Sept Order #0921.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 199.79.62.16
	DHL Express Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	0zWKZlSOqL.exe	Get hash	malicious	Browse	• 199.79.62.16
	ee5s192YZ34Ybve.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment advice_103.exe	Get hash	malicious	Browse	• 199.79.62.145
	QUOTATION.exe	Get hash	malicious	Browse	• 162.215.249.19
	diagram-595.doc	Get hash	malicious	Browse	• 116.206.10 5.115
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	• 208.91.199.224
	LJUNGBY QUOTATION.doc	Get hash	malicious	Browse	• 162.215.24 1.145
	TPL020321.doc	Get hash	malicious	Browse	• 162.215.24 1.145
	sapa list.doc	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bd0bf25947d4a37404f0424edf4db9ad	4GjwZxgraf.exe	Get hash	malicious	Browse	• 20.190.160.131
	hWEV7WHuSm.exe	Get hash	malicious	Browse	• 20.190.160.131
	Wire Payment-remittance#.html	Get hash	malicious	Browse	• 20.190.160.131
	securemessage.htm	Get hash	malicious	Browse	• 20.190.160.131
	oGgH8vgU0Z.exe	Get hash	malicious	Browse	• 20.190.160.131
	btweb_installer.exe	Get hash	malicious	Browse	• 20.190.160.131
	codes.zip.exe	Get hash	malicious	Browse	• 20.190.160.131
	r6.zip.exe	Get hash	malicious	Browse	• 20.190.160.131
	installer_20f7d5a8ce373.exe	Get hash	malicious	Browse	• 20.190.160.131
	eQjZ5OS5m5.exe	Get hash	malicious	Browse	• 20.190.160.131
	vape_all_versions.zip.exe	Get hash	malicious	Browse	• 20.190.160.131
	script_hack_412.zip.exe	Get hash	malicious	Browse	• 20.190.160.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DesktopCentralAgent.exe	Get hash	malicious	Browse	• 20.190.160.131
	orbi-valorant-injector.exe	Get hash	malicious	Browse	• 20.190.160.131
	Agenda1.docx	Get hash	malicious	Browse	• 20.190.160.131
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 20.190.160.131
	FragCache Hack v47.zip.exe	Get hash	malicious	Browse	• 20.190.160.131
	DesktopCentralAgent.exe	Get hash	malicious	Browse	• 20.190.160.131
	eBay-invoice-2195921.vbs	Get hash	malicious	Browse	• 20.190.160.131

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TOP URGENT.exe.log

Process:	C:\Users\user\Desktop\TOP URGENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.470825518995194

General

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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	TOP URGENT.exe
File size:	713216
MD5:	3af20ee616d2d9c806d27a3c245d4d7b
SHA1:	f4448544d0fd560be3a8c1e6ff46670251785267
SHA256:	c810e257ac876cb505d076efee941037f5f9fd11464a4af8515d0fbac61509b1
SHA512:	b1e98284ddc4e4ffb2742818e4a38c172d255a6922bd058b29f0fa0071c4564268e7faa967b6de4dc8713f322bf904afb801f58eee17d9d1e240f18f12b920ba
SSDEEP:	12288:i7kWHCM2K4CKI/yzQs2TaIpI0iJWRUB1acpCAIWoAdLekQNED0aoV5I:CE3CfMIpI0iJyUBnuW/vcEoaoV5I
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.Aa.....0..r...n..... .....@.. .....@.....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x4a90e2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6141B258 [Wed Sep 15 08:44:08 2021 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	0xa70e8	0xa7200	False	0.825526189697	data	7.54096955911	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x6b90	0x6c00	False	0.442672164352	data	5.09315736514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-16:23:28.117425	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49820	587	192.168.2.3	208.91.199.225

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 16:23:26.026834011 CEST	192.168.2.3	8.8.8.8	0x5147	Standard query (0)	smtp.almuntakhaba.com	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.557805061 CEST	192.168.2.3	8.8.8.8	0xd737	Standard query (0)	smtp.almuntakhaba.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 16:23:26.192635059 CEST	8.8.8.8	192.168.2.3	0x5147	No error (0)	smtp.almuntakhaba.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 16:23:26.192635059 CEST	8.8.8.8	192.168.2.3	0x5147	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.192635059 CEST	8.8.8.8	192.168.2.3	0x5147	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.192635059 CEST	8.8.8.8	192.168.2.3	0x5147	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.192635059 CEST	8.8.8.8	192.168.2.3	0x5147	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.717607021 CEST	8.8.8.8	192.168.2.3	0xd737	No error (0)	smtp.almuntakhaba.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 16:23:26.717607021 CEST	8.8.8.8	192.168.2.3	0xd737	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.717607021 CEST	8.8.8.8	192.168.2.3	0xd737	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.717607021 CEST	8.8.8.8	192.168.2.3	0xd737	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Sep 15, 2021 16:23:26.717607021 CEST	8.8.8.8	192.168.2.3	0xd737	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

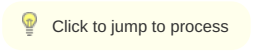
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 15, 2021 16:23:27.243478060 CEST	587	49820	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Sep 15, 2021 16:23:27.244544983 CEST	49820	587	192.168.2.3	208.91.199.225	EHLO 928100
Sep 15, 2021 16:23:27.388012886 CEST	587	49820	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Sep 15, 2021 16:23:27.389497042 CEST	49820	587	192.168.2.3	208.91.199.225	AUTH login cHBjQGFsbXVudGFraGFiYS5jb20=
Sep 15, 2021 16:23:27.533042908 CEST	587	49820	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
Sep 15, 2021 16:23:27.678124905 CEST	587	49820	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
Sep 15, 2021 16:23:27.679183006 CEST	49820	587	192.168.2.3	208.91.199.225	MAIL FROM:<ppc@almuntakhaba.com>
Sep 15, 2021 16:23:27.822444916 CEST	587	49820	208.91.199.225	192.168.2.3	250 2.1.0 Ok
Sep 15, 2021 16:23:27.822858095 CEST	49820	587	192.168.2.3	208.91.199.225	RCPT TO:<ppc@almuntakhaba.com>
Sep 15, 2021 16:23:27.972619057 CEST	587	49820	208.91.199.225	192.168.2.3	250 2.1.5 Ok
Sep 15, 2021 16:23:27.973043919 CEST	49820	587	192.168.2.3	208.91.199.225	DATA
Sep 15, 2021 16:23:28.116139889 CEST	587	49820	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Sep 15, 2021 16:23:28.118664980 CEST	49820	587	192.168.2.3	208.91.199.225	.
Sep 15, 2021 16:23:28.321346998 CEST	587	49820	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as DBF7FD96D1

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TOP URGENT.exe PID: 6352 Parent PID: 5424

General

Start time:	16:21:25
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\TOP URGENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TOP URGENT.exe'
Imagebase:	0x9f0000
File size:	713216 bytes
MD5 hash:	3AF20EE616D2D9C806D27A3C245D4D7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.244947880.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.245468332.0000000003D89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.245468332.0000000003D89000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: MSBuild.exe PID: 6592 Parent PID: 6352

General

Start time:	16:21:35
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0x690000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000004.00000002.501627918.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.501627918.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.493480561.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.493480561.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis