ID: 458887
Sample Name:
ORDER#142155312938
KALISKAYA WODKA
CON1GQDP- URGENT-
New.exe
Cookbook: default.jbs
Time: 20:42:33
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

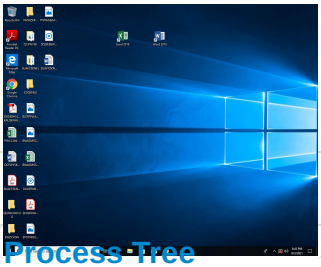
Windows Analysis Report ORDER#142155312938 KALIS…

Overview

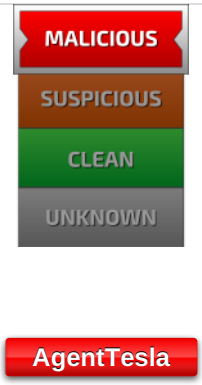
General Information

Sample Name:	ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
Analysis ID:	458887
MD5:	4eb106d21c787c..
SHA1:	2600e6b0ea8e3d..
SHA256:	9fcdd20c1848723..
Tags:	exe null
Infos:	

Most interesting Screenshot:



Detection

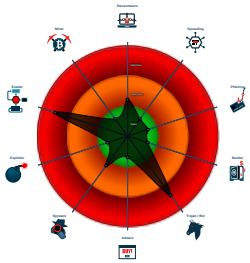


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains potentia…
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe (PID: 5748 cmdline: 'C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe' MD5: 4EB106D21C787C7B4215721673E15B39)
  - ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe (PID: 7008 cmdline: C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe MD5: 4EB106D21C787C7B4215721673E15B39)
- EnhancementRadio.exe (PID: 7104 cmdline: 'C:\Users\user\AppData\Local\EnhancementRadio.exe' MD5: 4EB106D21C787C7B4215721673E15B39)
- EnhancementRadio.exe (PID: 4308 cmdline: 'C:\Users\user\AppData\Local\EnhancementRadio.exe' MD5: 4EB106D21C787C7B4215721673E15B39)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "serena@mbalikova.com",
  "Password": "Pp88347521@",
  "Host": "mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.471689095.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000002.471689095.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.378683076.0000000003B78000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.378683076.0000000003B78000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000017.00000002.476536239.0000000002C1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.3c07d60.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.3c07d60.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.3bb7d40.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.3bb7d40.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.3c07d60.6.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 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 dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

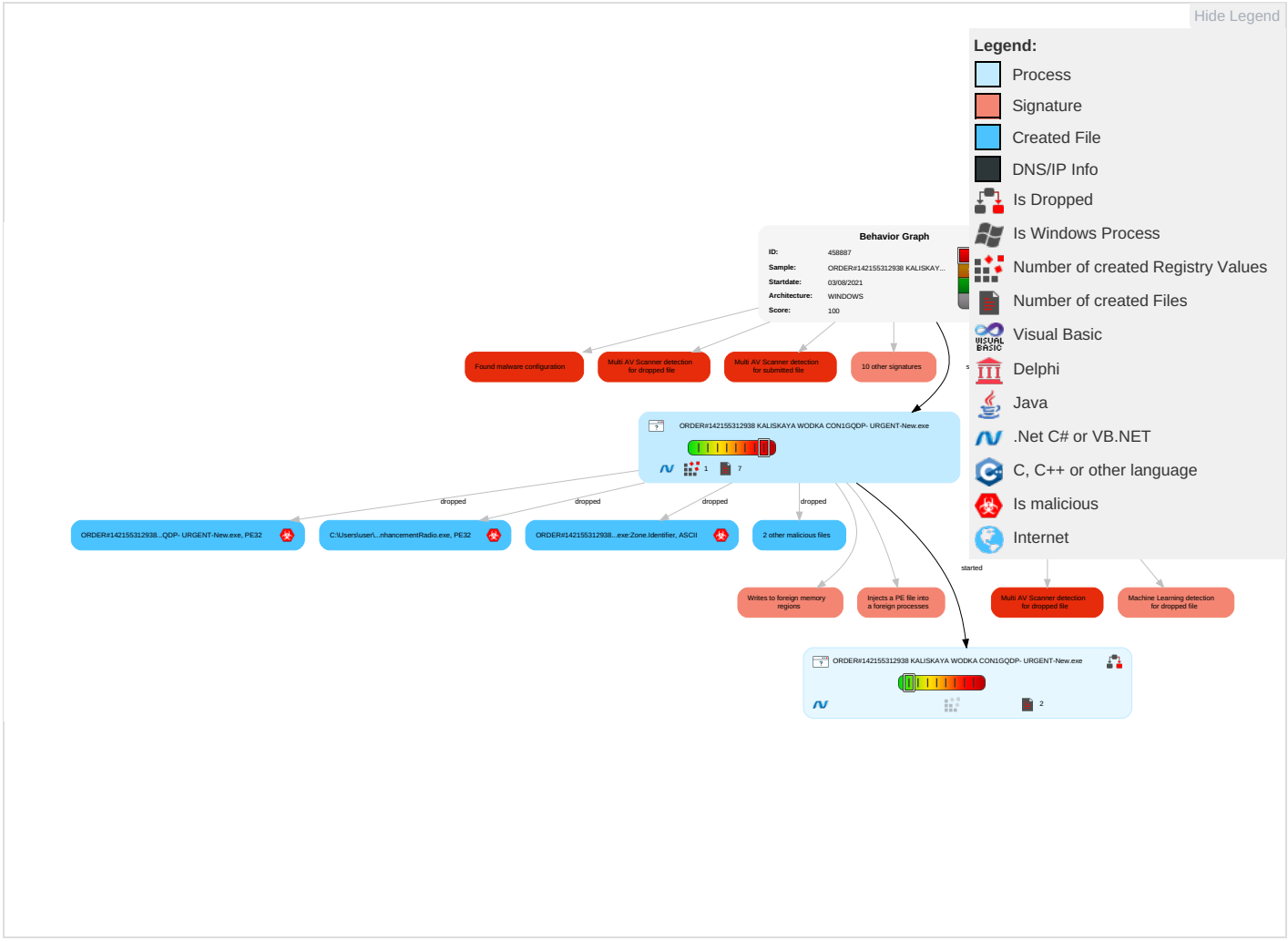
Yara detected AgentTesla

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	Registry Run Keys / Startup Folder 1	Process Injection 2 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 5 1	Security Account Manager	Virtualization/Sandbox Evasion 1 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	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	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

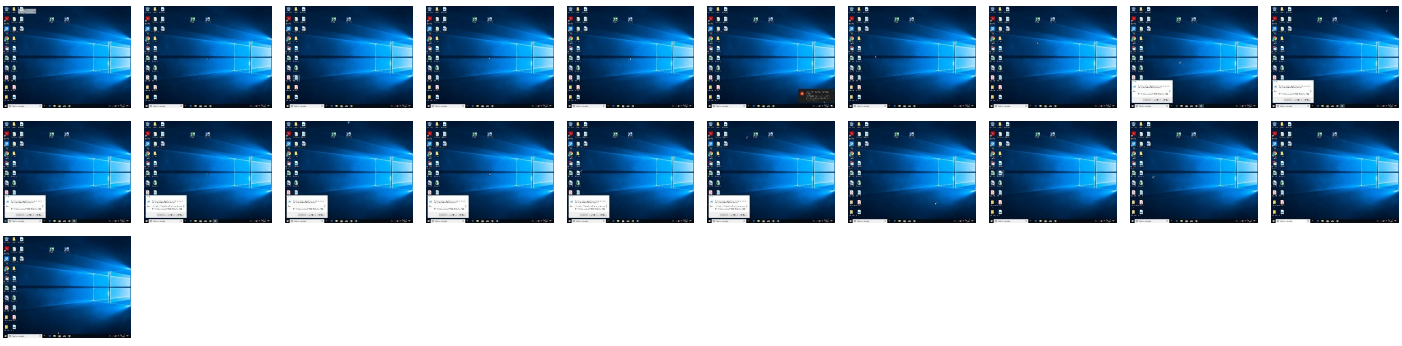
Behavior Graph



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
ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	63%	Virustotal		Browse
ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	46%	Metadefender		Browse
ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\EnhancementRadio.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EnhancementRadio.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\EnhancementRadio.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.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	
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://www.tiro.com	0%	URL Reputation	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://yFwcGw.com	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://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://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

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458887
Start date:	03.08.2021
Start time:	20:42:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.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.evad.winEXE@5/5@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • 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
20:44:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run EnhancementRadio "C:\Users\user\AppData\Local\EnhancementRadio.exe"
20:44:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run EnhancementRadio "C:\Users\user\AppData\Local\EnhancementRadio.exe"
20:44:51	API Interceptor	267x Sleep call for process: ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\EnhancementRadio.exe	
Process:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	584704
Entropy (8bit):	6.428997462356413
Encrypted:	false
SSDEEP:	12288:jb4ltZl87PVptm3TE8cCbUCOF1gJ3ntYJZ1iDwfUR8K:jbytZmBAbu1S9YJZJc
MD5:	4EB106D21C787C7B4215721673E15B39
SHA1:	2600E6B0EA8E3D39D4001ED0F8A35A87FC716566
SHA-256:	9FCDD20C1848723A889FD4EBB88E52A2CB9FAE8EC9E8CFE70D8E9706EF3E8992
SHA-512:	69BF8422C1102C6EE99139CB80070E0955D6B192DE831A577AE308A2460D5A52E975C358CA275A5E0015293A98ABA341BD7249842C073A911D34168B1B864A69
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 61%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..n...|..... .....@.. .....@..... ..@.....K.....x..... ....H.....text...4m... ...n..... ..`.rsrc....x.....z...p.....@..@.rel oc..... .....@..B.....H..... 4..8,.....X`...,.....^.(....8.....(....8....*.{....o....8.....0.....8}.....E....x...8s....{....o....s....%.. (....(....o....&8....*...X..8.... ....(....8.....{....o....s....%..(....o....o....&8h.....8V...8u...8.....?z...8!.....s....s....%o....o....8|..... ....~"...94...& ....8)...8....8-.. ....(....8G.....X..8.....? M...8.....0.....8....(.....o....*(.....o.....8.....{....(.....o..

C:\Users\user\AppData\Local\EnhancementRadio.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe.log	
Process:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, 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:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	
Process:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe

C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	584704
Entropy (8bit):	6.428997462356413
Encrypted:	false
SSDEEP:	12288:jb4ltZl87PVptm3TE8cCbUCOF1gJ3ntYJZ1iDwfUR8K:jbytZmBAbu1S9YJZJc
MD5:	4EB106D21C787C7B4215721673E15B39
SHA1:	2600E6B0EA8E3D39D4001ED0F8A35A87FC716566
SHA-256:	9FCDD20C1848723A889FD4EBB88E52A2CB9FAE8EC9E8CFE70D8E9706EF3E8992
SHA-512:	69BF8422C1102C6EE99139CB80070E0955D6B192DE831A577AE308A2460D5A52E975C358CA275A5E0015293A98ABA341BD7249842C073A911D34168B1B864A69
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 61%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..n...|..... .....@.. .....@..... ..@.....K.....x..... ....H.....text...4m... ...n..... ..`.rsrc....x.....z...p.....@..@.rel oc..... .....@..B.....H..... 4..8,.....X`...,.....^.(....8.....(....8....*r.(....8....*.{....o....8.....0.....8}.....E....x...8s....{....o....s....%.. (....(....o....&8....*...X..8.... ....(....8.....{....o....s....%..(....o....o....&8h.....8V...8u...8.....?z...8!.....s....s....%o....o....8|..... ....~"...94...& ....8)...8....8-.. ....(....8G.....X..8.....? M...8.....0.....8....(.....o....*(.....o.....8.....{....(.....o..

C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.428997462356413
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
File size:	584704
MD5:	4eb106d21c787c7b4215721673e15b39
SHA1:	2600e6b0ea8e3d39d4001ed0f8a35a87fc716566
SHA256:	9fcdd20c1848723a889fd4ebb88e52a2cb9fae8ec9e8cfe70d8e9706ef3e8992
SHA512:	69bf8422c1102c6ee99139cb80070e0955d6b192de831a577ae308a2460d5a52e975c358ca275a5e0015293a98ab a341bd7249842c073a911d34168b1b864a69
SSDEEP:	12288:jb4ltZl87PVptm3TE8cCbUCOF1gJ3ntYJZ1iDwfUR8K:jbytZmBAbu1S9YJZJc

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..n...|..... .....@.. .....@.....@.....

File Icon

Icon Hash:	60d8c8c9c9e9c1c8

Static PE Info

General

Entrypoint:	0x488d2e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xB5F6BF93 [Mon Sep 27 21:03:15 2066 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	0x86d34	0x86e00	False	0.70304716462	data	6.18965039171	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x78a4	0x7a00	False	0.887102971311	data	7.74086473521	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	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

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe PID: 5748 Parent PID: 5644

General

Start time:	20:43:22
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP-URGENT-New.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe'
Imagebase:	0x630000
File size:	584704 bytes
MD5 hash:	4EB106D21C787C7B4215721673E15B39
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: 00000001.00000002.378683076.0000000003B78000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.378683076.0000000003B78000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.378760193.0000000003C07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.378760193.0000000003C07000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.378128189.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.378128189.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.375822190.0000000002B18000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.375822190.0000000002B18000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe PID: 7008 Parent PID: 5748

General

Start time:	20:44:40
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CON1GQDP- URGENT-New.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ORDER#142155312938 KALISKAYA WODKA CO N1GQDP- URGENT-New.exe
Imagebase:	0x7f0000
File size:	584704 bytes
MD5 hash:	4EB106D21C787C7B4215721673E15B39
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: 00000017.00000002.471689095.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.471689095.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.476536239.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 61%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: EnhancementRadio.exe PID: 7104 Parent PID: 3388

General

Start time:	20:44:50
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\EnhancementRadio.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\EnhancementRadio.exe'
Imagebase:	0x660000
File size:	584704 bytes
MD5 hash:	4EB106D21C787C7B4215721673E15B39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, Metadefender, Browse • Detection: 61%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: EnhancementRadio.exe PID: 4308 Parent PID: 3388

General

Start time:	20:44:59
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Local\EnhancementRadio.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\EnhancementRadio.exe'
Imagebase:	0x550000
File size:	584704 bytes
MD5 hash:	4EB106D21C787C7B4215721673E15B39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis