ID: 458837
Sample Name: model 800 DD.exe
Cookbook: default.jbs
Time: 19:35:42
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

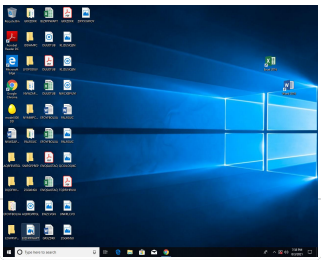
Windows Analysis Report model 800 DD.exe

Overview

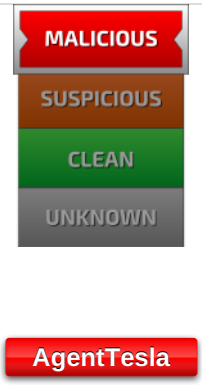
General Information

Sample Name:	model 800 DD.exe
Analysis ID:	458837
MD5:	d7191bd9419ce6..
SHA1:	7b847b776a23dff..
SHA256:	bb422900a755e4..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

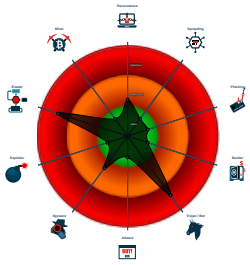


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg…
- Hides that the sample has been dow…
- 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**
- model 800 DD.exe (PID: 2848 cmdline: 'C:\Users\user\Desktop\model 800 DD.exe' MD5: D7191BD9419CE60F57122E0A3B6D8449)
  - model 800 DD.exe (PID: 5840 cmdline: C:\Users\user\Desktop\model 800 DD.exe MD5: D7191BD9419CE60F57122E0A3B6D8449)
  - model 800 DD.exe (PID: 4276 cmdline: C:\Users\user\Desktop\model 800 DD.exe MD5: D7191BD9419CE60F57122E0A3B6D8449)
  - model 800 DD.exe (PID: 4632 cmdline: C:\Users\user\Desktop\model 800 DD.exe MD5: D7191BD9419CE60F57122E0A3B6D8449)
- rmKknnU.exe (PID: 5732 cmdline: 'C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe' MD5: D7191BD9419CE60F57122E0A3B6D8449)
  - rmKknnU.exe (PID: 4944 cmdline: C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe MD5: D7191BD9419CE60F57122E0A3B6D8449)
- rmKknnU.exe (PID: 5592 cmdline: 'C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe' MD5: D7191BD9419CE60F57122E0A3B6D8449)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "accounts@alexfoxfreight.com",
  "Password": "Ueos*93sj!#!12",
  "Host": "mail.alexfoxfreight.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.495139244.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.495139244.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.500269130.0000000002C01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.500269130.0000000002C0 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000002.495247778.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.model 800 DD.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.model 800 DD.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
22.2.rmKknnU.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
22.2.rmKknnU.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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

Networking:

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

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

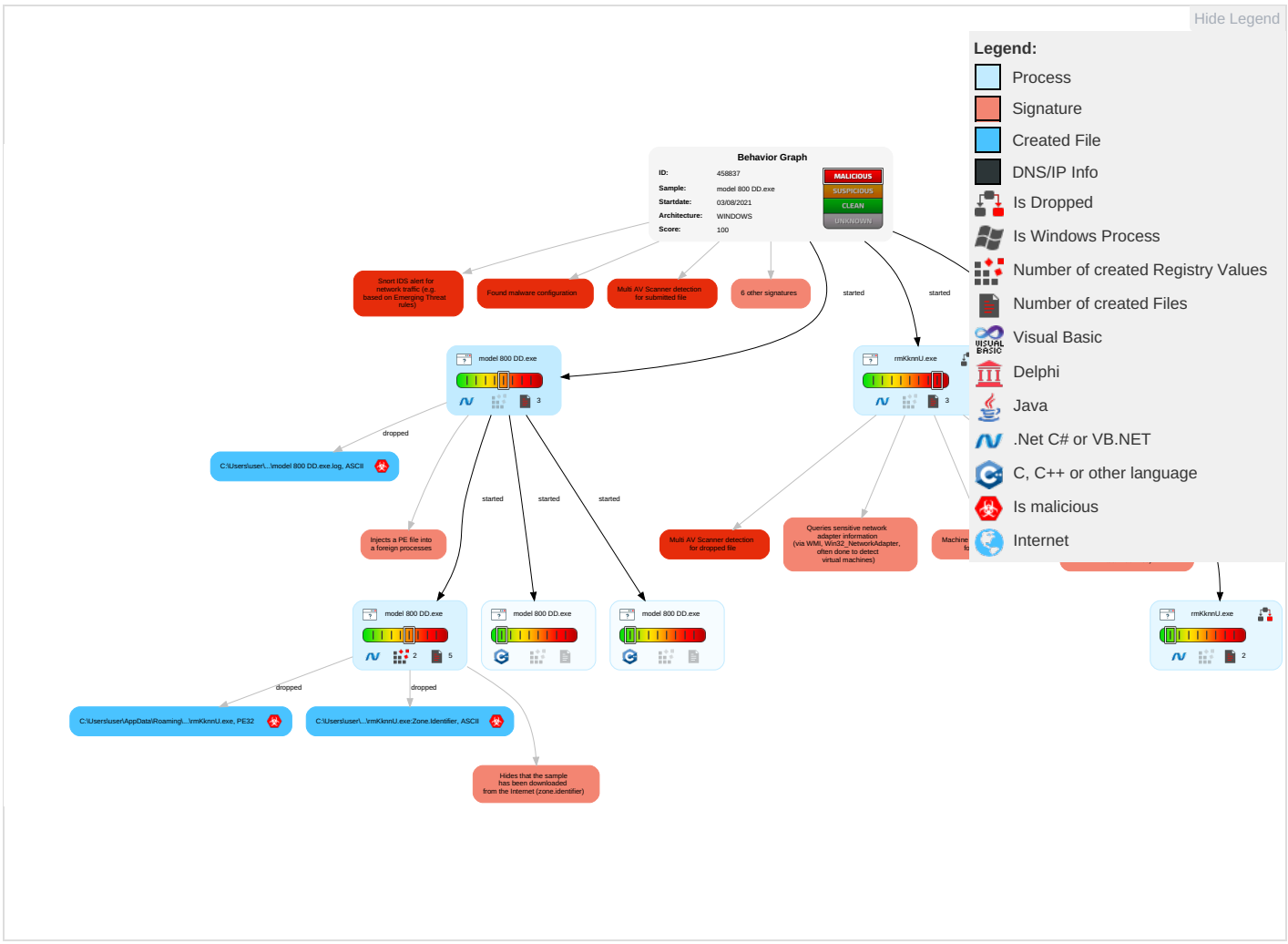
Yara detected AgentTesla

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 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 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	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 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 1 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 1 3	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	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

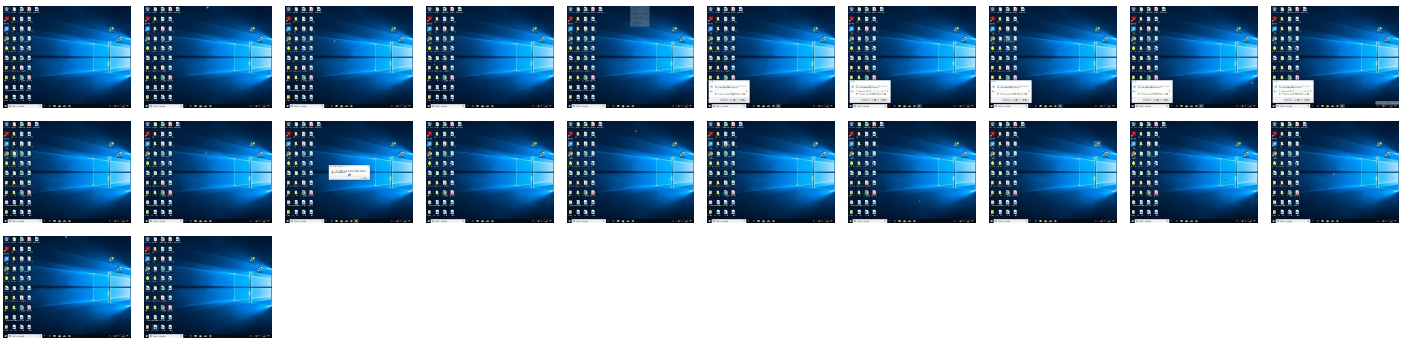
Behavior Graph



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
model 800 DD.exe	36%	Virustotal		Browse
model 800 DD.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	
model 800 DD.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe	36%	Virustotal		Browse
C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe	77%	ReversingLabs	ByteCode-MSIL.Trojan.AgenteslaPacker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.model 800 DD.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.2.rmKknnU.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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://BYnWgg.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	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://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

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:	458837
Start date:	03.08.2021
Start time:	19:35:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	model 800 DD.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:	27
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@11/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 23% • Quality standard deviation: 32.5%
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
19:36:52	API Interceptor	616x Sleep call for process: model 800 DD.exe modified
19:37:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run rmKknnU C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
19:37:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run rmKknnU C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
19:37:56	API Interceptor	215x Sleep call for process: rmKknnU.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\Microsoft\CLR_v4.0_32\UsageLogs\model 800 DD.exe.log	
Process:	C:\Users\user\Desktop\model 800 DD.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\model 800 DD.exe.log	
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\Microsoft\CLR_v4.0_32\UsageLogs\rmKknnU.exe.log	
Process:	C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.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:	false
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:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe	
Process:	C:\Users\user\Desktop\model 800 DD.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1348608
Entropy (8bit):	7.538212963459183
Encrypted:	false
SSDEEP:	24576:xKjE76DODfx8Dgyfx8DgJTs5SjywMd6s38Yx8FwDZyfL:EE76+58Dgy58DgJI5SjyEsMYFZ6
MD5:	D7191BD9419CE60F57122E0A3B6D8449
SHA1:	7B847B776A23DFF9FA06429F7AB6BF05A27CF51C
SHA-256:	BB422900A755E4AA68626B1451545A2E36E1ACF79D975AE6BDA7DA78313C3205
SHA-512:	92F48500661FCC1C54E949669A63E149B0AE57B7D8E7BFF5CAC5A92445E6D1FCCE7D16F319CF054DD376756EA317A53BCF7D79E8C9E679530919C4B0FAEF92I 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 36%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^..a.....P.....>.... .....@.. ....@.....O.....@..... ....H.....text...D.... ....`.rsrc...@.....@..@.rel oc.....@..B..... .....H.....0.....s.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\model 800 DD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe:Zone.Identifier	
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):	7.538212963459183
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:	model 800 DD.exe
File size:	1348608
MD5:	d7191bd9419ce60f57122e0a3b6d8449
SHA1:	7b847b776a23dff9fa06429f7ab6bf05a27cf51c
SHA256:	bb422900a755e4aa68626b1451545a2e36e1acf79d975ae6bda7da78313c3205
SHA512:	92f48500661fcc1c54e949669a63e149b0ae57b7d8e7bff5cac5a92445e6d1fcce7d16f319cf054dd376756ea317a53bcf7d79e8c9e679530919c4b0faef92b8
SSDEEP:	24576:xKjE76DODfx8Dgyfx8DgJTs5SjywMd6s38Yx8FwDZyfL:EE76+58Dgy58DgJl5SjyEsMYFZ6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^...a.....P.....>.... ....@.. .....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x53d73e
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:	0x6108075E [Mon Aug 2 14:55:26 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	0x13b744	0x13b800	False	0.713922902635	data	7.57001311304	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x13e000	0xd640	0xd800	False	0.708586516204	data	6.59878641909	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14c000	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: model 800 DD.exe PID: 2848 Parent PID: 5664

General

Start time:	19:36:33
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\model 800 DD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\model 800 DD.exe'
Imagebase:	0xd30000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
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 Written

File Read

Analysis Process: model 800 DD.exe PID: 5840 Parent PID: 2848

General

Start time:	19:36:53
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\model 800 DD.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\model 800 DD.exe
Imagebase:	0x310000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: model 800 DD.exe PID: 4276 Parent PID: 2848

General

Start time:	19:36:54
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\model 800 DD.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\model 800 DD.exe
Imagebase:	0x3d0000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: model 800 DD.exe PID: 4632 Parent PID: 2848

General

Start time:	19:36:55
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\model 800 DD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\model 800 DD.exe
Imagebase:	0x760000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
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: 00000006.00000002.500269130.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.500269130.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.495247778.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.495247778.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: rmKknnU.exe PID: 5732 Parent PID: 3472

General

Start time:	19:37:27
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe'
Imagebase:	0x920000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, Virustotal, Browse • Detection: 77%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: rmKknnU.exe PID: 5592 Parent PID: 3472

General

Start time:	19:37:35

Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe'
Imagebase:	0x6c0000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
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

Analysis Process: rmKknnU.exe PID: 4944 Parent PID: 5732

General

Start time:	19:37:57
Start date:	03/08/2021
Path:	C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rmKknnU\rmKknnU.exe
Imagebase:	0xaf0000
File size:	1348608 bytes
MD5 hash:	D7191BD9419CE60F57122E0A3B6D8449
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: 00000016.00000002.495139244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000002.495139244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.499443817.0000000003061000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.499443817.0000000003061000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis