ID: 345042
Sample Name:
SecuriteInfo.com.Trojan.MulDrop16.9965.2278.18780
Cookbook: default.jbs
Time: 16:14:38
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Trojan.MulDrop16.9965.2278.18780 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
System Summary: 5
Boot Survival: 5
Malware Analysis System Evasion: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 11
General 11
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 11
Data Directories 13
Sections 13
Resources 13
Imports 14
Version Infos 14
Network Behavior 14
Code Manipulations 14

Statistics 14
Behavior 14
System Behavior 14
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5660 Parent PID: 5532 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
File Read 17
Analysis Process: schtasks.exe PID: 4864 Parent PID: 5660 17
General 17
File Activities 18
File Read 18
Analysis Process: conhost.exe PID: 4700 Parent PID: 4864 18
General 18
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5456 Parent PID: 5660 18
General 18
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 852 Parent PID: 5660 19
General 19
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5948 Parent PID: 5660 19
General 19
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5796 Parent PID: 5660 19
General 19
Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 1368 Parent PID: 5660 19
General 20
Disassembly 20
Code Analysis 20

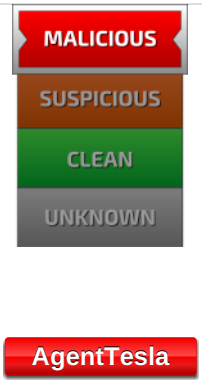
Analysis Report SecuriteInfo.com.Trojan.MulDrop16.996…

Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.MulDrop16.9965.2278.18780 (renamed file extension from 18780 to exe)
Analysis ID:	345042
MD5:	e750511892ab53..
SHA1:	d78aa528d38fa57.
SHA256:	4328e4ac330339..

Detection

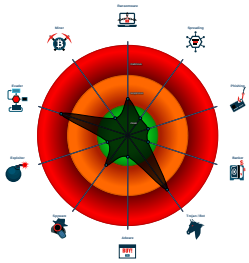


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Uses schtasks.exe or at.exe to add …
- Contains capabilities to detect virtua…
- Contains functionality to detect virtu…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 5660 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe' MD5: E750511892AB532FB2147F4537DABCFD)
  - schtasks.exe (PID: 4864 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XdwuEt' /XML 'C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp' MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 4700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 5456 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe MD5: E750511892AB532FB2147F4537DABCFD)
  - SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 852 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe MD5: E750511892AB532FB2147F4537DABCFD)
  - SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 5948 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe MD5: E750511892AB532FB2147F4537DABCFD)
  - SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 5796 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe MD5: E750511892AB532FB2147F4537DABCFD)
  - SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe (PID: 1368 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe MD5: E750511892AB532FB2147F4537DABCFD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.225631461.0000000002DD1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.225667409.0000000002E28000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.226077491.0000000012DE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

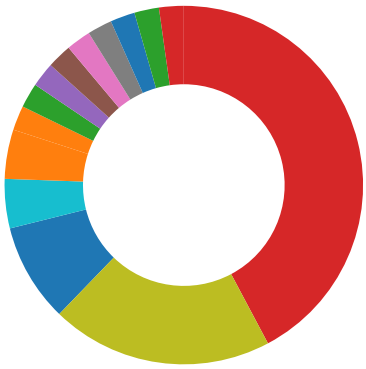
Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5660	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5660	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

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

Compliance:

Contains modern PE file flags such as dynamic base (ASLR) or NX

System Summary:

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Stealing of Sensitive Information:

Yara detected AgentTesla

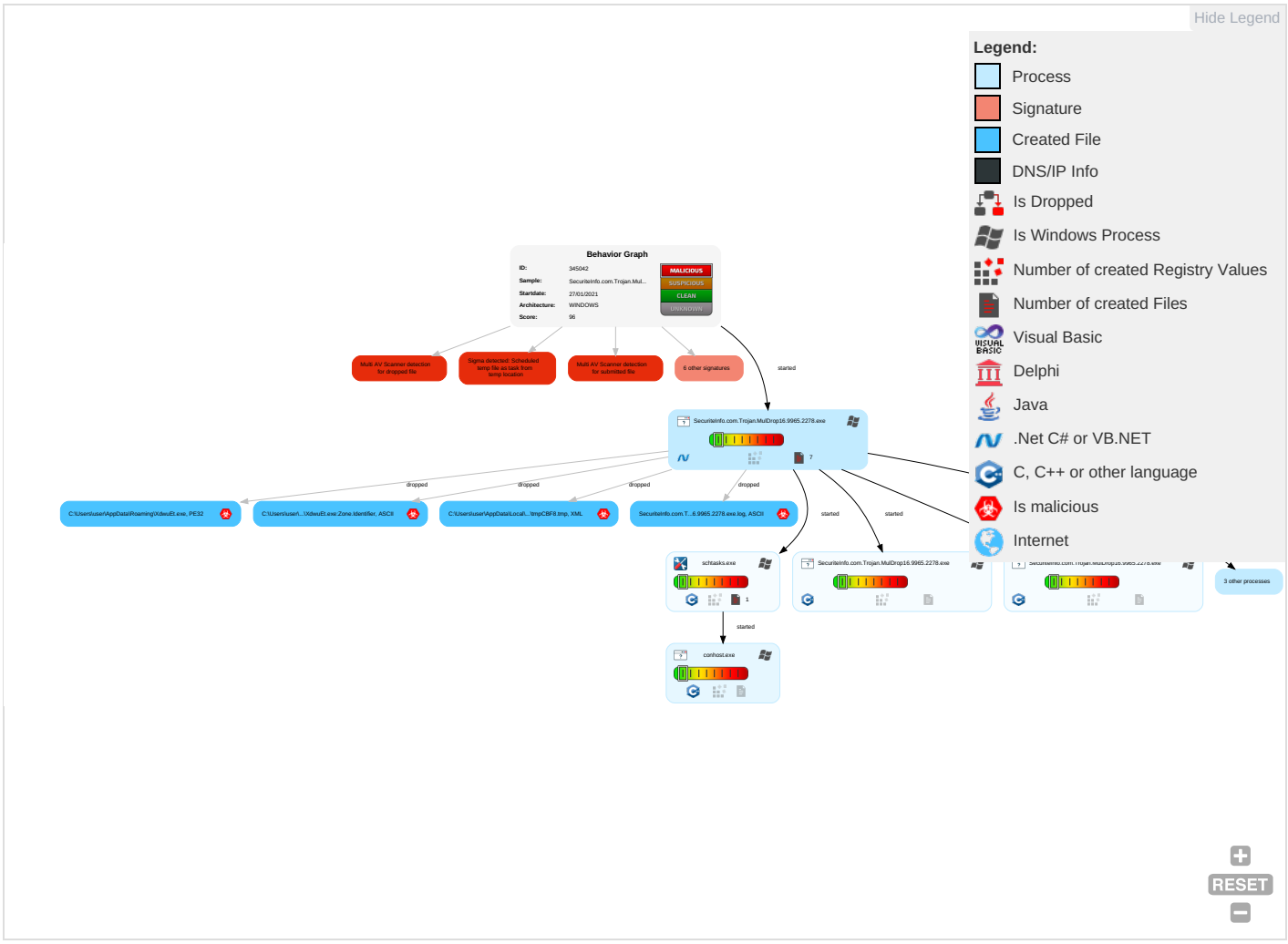
Remote Access Functionality:

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	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe	35%	Virustotal		Browse
SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\XdwuEt.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\XdwuEt.exe	35%	Virustotal		Browse
C:\Users\user\AppData\Roaming\XdwuEt.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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	
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

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe, 00000000.000000002.225631461.0000000002DD1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe, 00000000.000000002.226077491.0000000012DE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345042
Start date:	27.01.2021
Start time:	16:14:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.MulDrop16.9965.2278.18780 (renamed file extension from 18780 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:	8
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:	mal96.troj.evad.winEXE@14/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.5% (good quality ratio 2.5%) • Quality average: 31% • Quality standard deviation: 32.2%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:15:31	API Interceptor	2x Sleep call for process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.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\UsageLogs\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1742
Entropy (8bit):	5.381353871108486
Encrypted:	false
SSDEEP:	48:MxHKEYHKGD8Ao6+vxpNl1qHGiD0HKeGitHTG1hAHKKPJAmHKoA9:iqEYqGgAo9ZPlwmI0qertzG1eqKPJ/qT
MD5:	978918F6120A43D1FA5899938A5A542F
SHA1:	6567A2E687B40BFD3A46246F51F4C89D93D89455
SHA-256:	F814F290A540B3FD755D05F3434317D7B26F2C33D2087F9E63233CD88AB510FC
SHA-512:	1DF2AF5A3F8212BF591AAA366FE96F167F3E6D43746E07B7CD44F1B2F06C63B1D290412891AD0B4D0A82D1DFD6EB2EB7D70981C35941F370DC97729E9205DD5
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_6

C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.184744549823039
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBLQrtn:cbh47TlNQ//rydbz9I3YODOLNdq3NQp
MD5:	90BBB757FD516A98CE985F615199C9C5
SHA1:	D17490C1D27995F6B68F137D14E6732A3E156C2C
SHA-256:	C90368DA6B08D81AF46467FCD1F37550E9A11393DFDFBE0FBE372C61416D1708
SHA-512:	EF79D2570DF43FF1BB12E049D49286BB3011BE58203E48FEDF283AB31DC0E5F358B86806D1E2B8A73436A313C26720C5EBEE4AA0E552C81E357D6D657287450
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\XdwuEt.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	541184
Entropy (8bit):	7.789762421792232
Encrypted:	false
SSDEEP:	12288:jgDW4PmoO4lv8zw7n9AXJBkwVHI3eC9Z9rzWmvRM:L4uoO4VnsJRHc/zJ
MD5:	E750511892AB532FB2147F4537DABCFD
SHA1:	D78AA528D38FA57BD3A5BF591CBD4437EBCDF377
SHA-256:	4328E4AC330339D884B95D99128404D4F8B5D6B695A9F583FF4C3F3A61AC4FF8
SHA-512:	F0C1AF9E1B8175EA91337702FFA8140DD0C901C8AC570A1DEF1299F2493EFC6FD66F36E19C8AE6B1B5C2B0F174A44A8754761A30EB2E652F3FC2E8D90A939BD5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....".....P..6.....U... ...`....@.. ....@.....tU..O....`..`..... ....H.....text....5... ...6..... ..`.rsrc...`....`.....8.....@..@.reloc.....@.....@..B.....U.....H.....\|.....,...H.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o....(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Roaming\XdwuEt.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.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

C:\Users\user\AppData\Roaming\XdwuEt.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.789762421792232
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:	SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
File size:	541184
MD5:	e750511892ab532fb2147f4537dabcfd
SHA1:	d78aa528d38fa57bd3a5bf591cbd4437ebcdf377
SHA256:	4328e4ac330339d884b95d99128404d4f8b5d6b695a9f583ff4c3f3a61ac4ff8
SHA512:	f0c1af9e1b8175ea91337702ffa8140dd0c901c8ac570a1def1299f2493efc6fd66f36e19c8ae6b1b5c2b0f174a44a8754761a30eb2e652f3fc2e8d90a939bd5
SSDEEP:	12288:jgDW4PmoO4lv8zw7n9AXJBkwVHI3eC9Z9rzWmvRM:L4uoO4VnsJRHc/zJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....".P..6.....U... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4855c6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x601113D8 [Wed Jan 27 07:18:48 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x85574	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x660	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x835cc	0x83600	False	0.878449096099	data	7.80365257713	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x660	0x800	False	0.3466796875	data	3.54395993413	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x86090	0x3d0	data		
RT_MANIFEST	0x86470	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Steffen Henjes
Assembly Version	0.2.0.0
InternalName	LocalActivator.exe
FileVersion	0.2.0.0
CompanyName	www.steffen-blogging.de
LegalTrademarks	
Comments	
ProductName	Dummy File Creator - powered by steffen-blogging.de
ProductVersion	0.2.0.0
FileDescription	DFC - Dummy File Creator
OriginalFilename	LocalActivator.exe

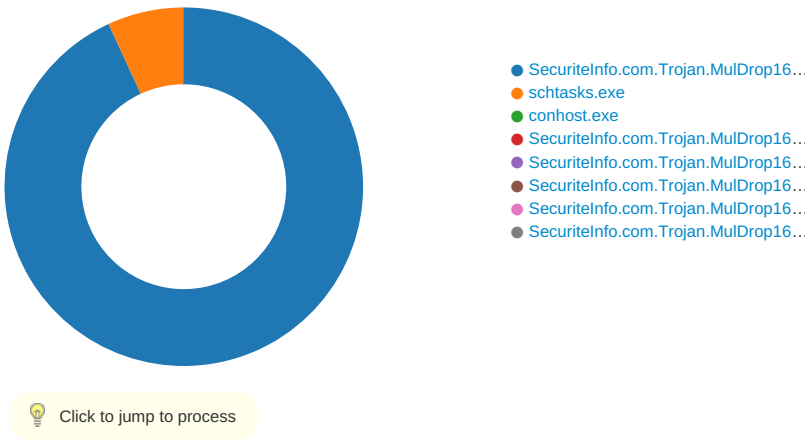
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5660
Parent PID: 5532

General

Start time:	16:15:30
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe'
Imagebase:	0x980000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
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: 00000000.00000002.225631461.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.225667409.0000000002E28000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.226077491.0000000012DE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4D84F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4D84F1E9	unknown
C:\Users\user\AppData\Roaming\XdwuEt.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFB4CD5817A	CopyFileW
C:\Users\user\AppData\Roaming\XdwuEt.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFB4CD5817A	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFB4C67F0F1	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB4DCB86ED	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	success or wait	1	7FFB4C67F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\XdwuEt.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 d8 13 11 60 00 00 00 00 00 00 00 e0 00 22 00 0b 01 50 00 00 36 08 00 00 0a 00 00 00 00 00 00 c6 55 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L.....`..... "...P..6.....U... ...`....@.. ....@.....	success or wait	3	7FFB4CD5817A	CopyFileW
C:\Users\user\AppData\Roaming\XdwuEt.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	7FFB4CD5817A	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	unknown	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	7FFB4C67B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe.log	unknown	1742	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	7FFB4DCB8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D71B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4D71B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D722625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4D7F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4D71B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4D71B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4C67B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4C67B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runt73a1fc9d#\41851b65542a0ba8b838baf0509a4554\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	7FFB4D7F12E7	ReadFile

Analysis Process: schtasks.exe PID: 4864 Parent PID: 5660

General

Start time:	16:15:32
Start date:	27/01/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XdwuEt' /XML 'C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp'
Imagebase:	0x7ff634190000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	unknown	2	success or wait	1	7FF63419A3B6	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCBF8.tmp	unknown	1640	success or wait	1	7FF63419A4AD	ReadFile

Analysis Process: conhost.exe PID: 4700 Parent PID: 4864

General

Start time:	16:15:33
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5456 Parent PID: 5660

General

Start time:	16:15:33
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Imagebase:	0x900000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 852 Parent PID: 5660

General

Start time:	16:15:34
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Imagebase:	0x170000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5948 Parent PID: 5660

General

Start time:	16:15:34
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Imagebase:	0xe90000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 5796 Parent PID: 5660

General

Start time:	16:15:35
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Imagebase:	0x6e0000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe PID: 1368 Parent PID: 5660

General

Start time:	16:15:35
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MulDrop16.9965.2278.exe
Imagebase:	0xf30000
File size:	541184 bytes
MD5 hash:	E750511892AB532FB2147F4537DABCFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis