

ID: 320546
Sample Name: SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.10025
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:16:56
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.10025 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 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
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 9
Static OLE Info 9
General 10
OLE File "SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls" 10
Indicators 10
Summary 10
Document Summary 10
Streams 10
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 10
General 10
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 10
General 10
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 405135 11
General 11
Network Behavior 11
Code Manipulations 11
Statistics 11

System Behavior 11
Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584 11
General 11
File Activities 11
Registry Activities 12
Disassembly 12

Copyright null 2020

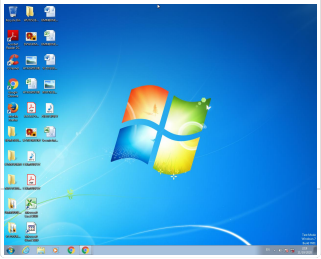
Analysis Report SecuriteInfo.com.Macro.Trojan-Downlo…

Overview

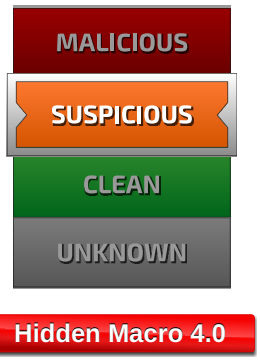
General Information

Sample Name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.10025 (renamed file extension from 10025 to xls)
Analysis ID:	320546
MD5:	66de86a7d9ba80..
SHA1:	8c0dcef8ad7aeb1..
SHA256:	bc3b0df0a90971d.

Most interesting Screenshot:



Detection



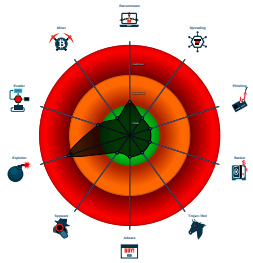
Hidden Macro 4.0

Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Yara detected password protected x…
- Unable to load, office file is protecte…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1748 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

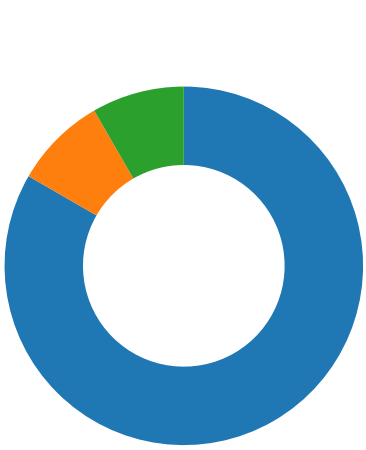
Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls	JoeSecurity_PasswordProtectedXlsWithEmbeddedMacros	Yara detected password protected xls with embedded macros	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

HIPS / PFW / Operating System Protection Evasion:

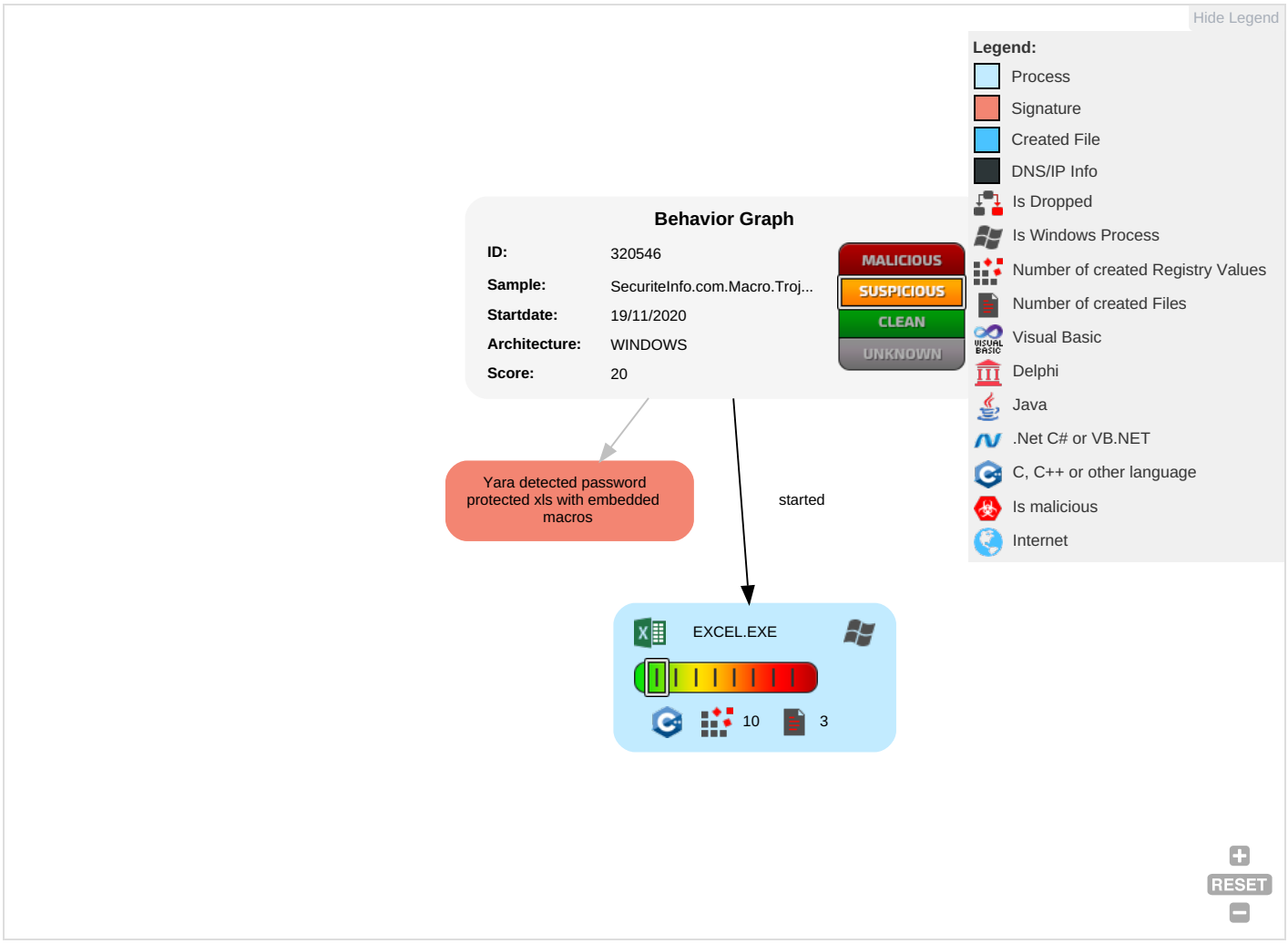


Yara detected password protected xls with embedded macros

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

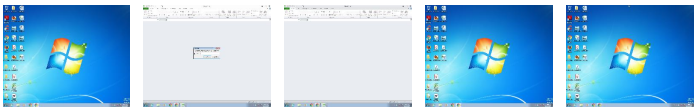
Behavior Graph



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.Macro.Trojan-Downloader.Encrypted.A.xls	6%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright null 2020

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320546
Start date:	19.11.2020
Start time:	14:16:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.10025 (renamed file extension from 10025 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus20.expl.winXLS@1/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Changed system and user locale, location and keyboard layout to Italian - Italy • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: bOpMKmUlXbBbmg, Last Saved By: administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Nov 18 22:00:31 2020, Last Saved Time/Date: Wed Nov 18 23:17:00 2020, Security: 1
Entropy (8bit):	7.6578858889050165
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls
File size:	418304
MD5:	66de86a7d9ba80c175fe166a81d25c4d
SHA1:	8c0dcef8ad7aeb1e77bc8a18f19d270af61c94e3
SHA256:	bc3b0df0a90971d83f87af531671216d238ce21b6272aa2758b178cbb1320276
SHA512:	c7b1885f70898bf90e677962c595df8d6d1a7b840a9c14647957726c59f67c4b8073c1a2289143dca6e92b58ec9f32e574b6f365c5315500c7eee3eeec6bd8a6
SSDEEP:	12288:t6Qtw5NtDtkd1zsRXSqUXVIF/MZX3BhAOepArPmHQeq:G5bpY1zstSNXuVKX4OepArMJq
File Content Preview:	.....>...../.....(...)...*....+...,...-.....

File Icon



Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Macro.Trojan-Downloader.Encrypted.A.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary	
Code Page:	1252
Author:	bOpMKmUlXbBbmg
Last Saved By:	administrator
Create Time:	2020-11-18 22:00:31
Last Saved Time:	2020-11-18 23:17:00
Creating Application:	Microsoft Excel
Security:	1

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.839708850949
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . L . . . . . P . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . F o g l i o 1 . . . . . F o g l i o 2 . . . . F o g l i o 3 . . . . . F o g l i o 4 . . . . . E T M v d g B d
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 4c 02 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 01 02 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.327276850068
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . ` . . . . . x . . . . . b O p M K m U l X b B b r g . . . . . a d m i n i s t r a t o r . . . . . M i c r o s o f t E x c e l . @ . . . . . c ; . . . . @ . . . . ~ . . . . .

General	
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 b0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 78 00 00 00 0c 00 00 00 90 00 00 00 0d 00 00 00 9c 00 00 00 13 00 00 00 a8 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 405135

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	405135
Entropy:	7.75501180979
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . / . . . . . ~ . . . . . h . . . . . M . i c . r . o . s . o . f . t . . E . n . h . a . n . c . e . d . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . v . 1 . . . 0 . . . . . D . I r " . . . v f \ \ . W p . . . . . t . . - . . . 1 . . . . . . m . . . 7 F V - . ! .) . # . . . . . \ \ . p . . . . . 7 . * . ` . / .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 2f 00 c8 00 01 00 04 00 02 00 0c 00 00 00 7e 00 00 00 0c 00 00 00 00 00 00 00 01 68 00 00 04 80 00 00 80 00 00 00 01 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584

General

Start time:	14:17:45
Start date:	19/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f350000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Copyright null 2020