ID: 528587
Sample Name: survey-1384723731.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:30:13
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report survey-1384723731.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Dropped Files 4
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
Software Vulnerabilities: 5
System Summary: 5
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 URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 13
File Icon 13
Static OLE Info 13
General 13
OLE File "survey-1384723731.xls" 13
Indicators 13
Summary 13
Document Summary 13
Streams 14
Macro 4.0 Code 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
HTTP Request Dependency Graph 14
HTTPS Proxied Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 16
Analysis Process: EXCEL.EXE PID: 408 Parent PID: 596 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Moved 16
Registry Activities 16
Key Created 16

Key Value Created 16
Key Value Modified 16
Analysis Process: regsvr32.exe PID: 2192 Parent PID: 408 16
General 16
File Activities 16
Analysis Process: regsvr32.exe PID: 2604 Parent PID: 408 16
General 17
File Activities 17
Analysis Process: regsvr32.exe PID: 1184 Parent PID: 408 17
General 17
File Activities 17
Disassembly 17
Code Analysis 17

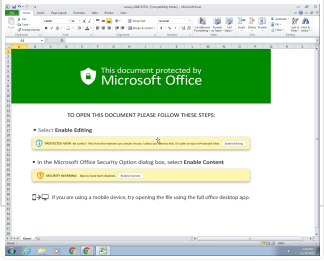
Windows Analysis Report survey-1384723731.xls

Overview

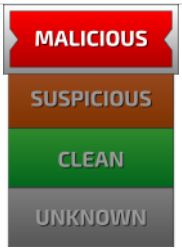
General Information

Sample Name:	survey-1384723731.xls
Analysis ID:	528587
MD5:	00bec62d14bc9f8..
SHA1:	d2ef80f029f8f035..
SHA256:	59d14a53849a19..
Infos:	

Most interesting Screenshot:



Detection



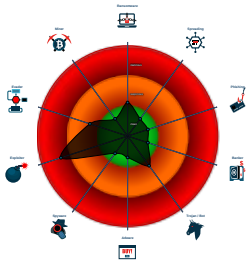
Hidden Macro 4.0

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Yara signature match
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 408 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2192 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\besta.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2604 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestb.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1184 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
survey-1384723731.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x3b2aa:$s1: Excel • 0x3c378:$s1: Excel • 0x3521:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 01 3A
survey-1384723731.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\survey-1384723731.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x3b2aa:$s1: Excel • 0x3c378:$s1: Excel • 0x3521:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 01 3A

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\survey-1384723731.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

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)

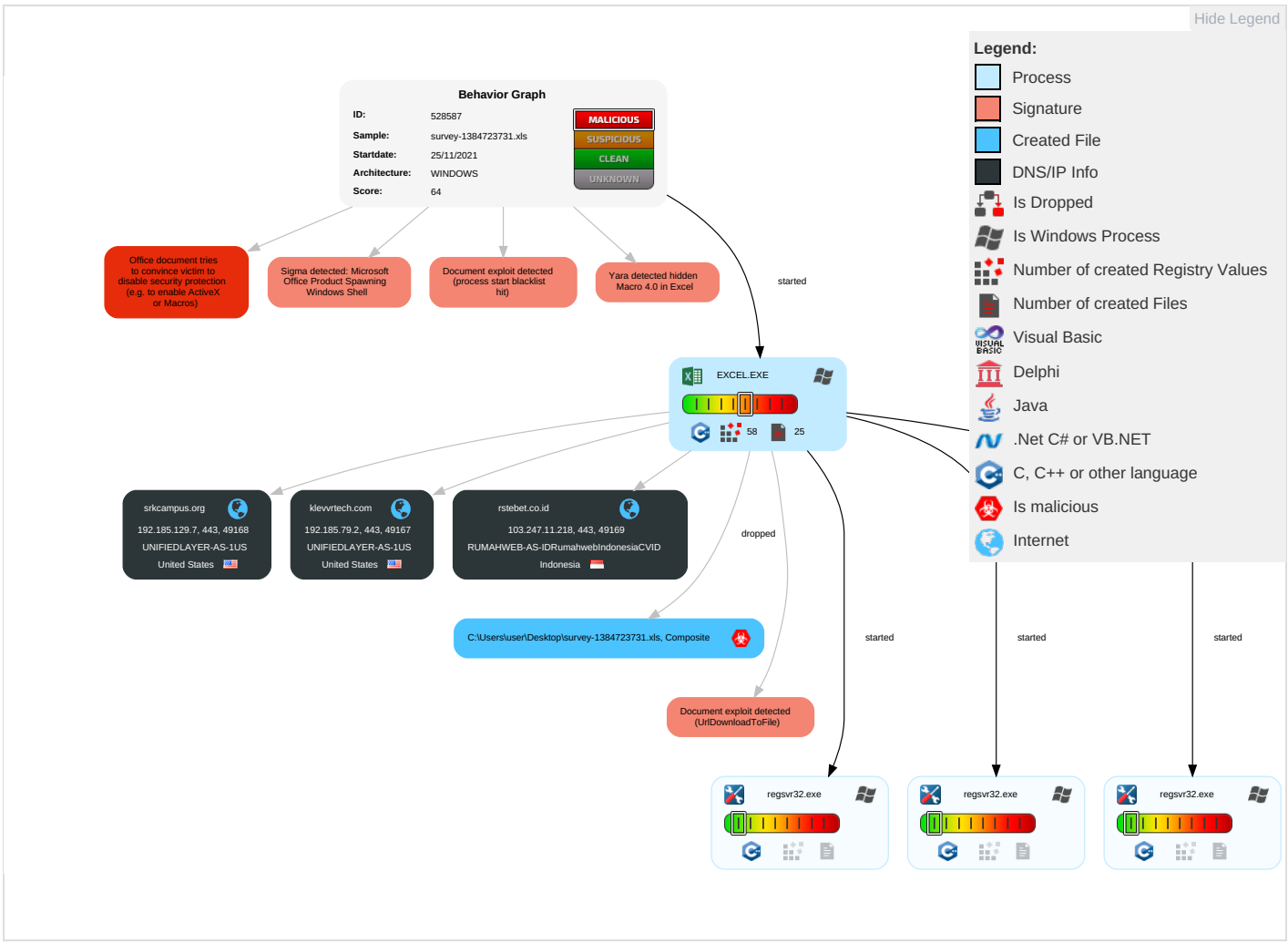
HIPS / PFW / Operating System Protection Evasion:

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 El
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 2	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 3	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 2	SIM Card Swap	

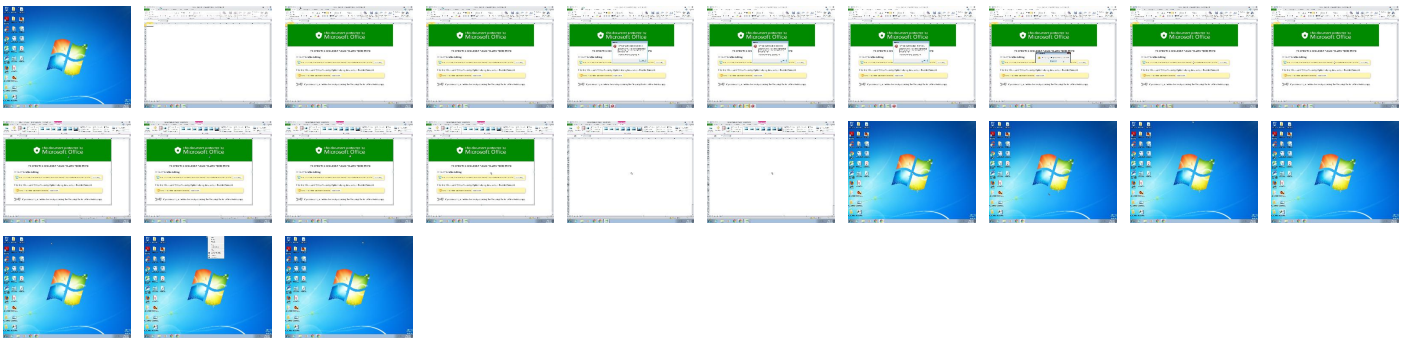
Behavior Graph

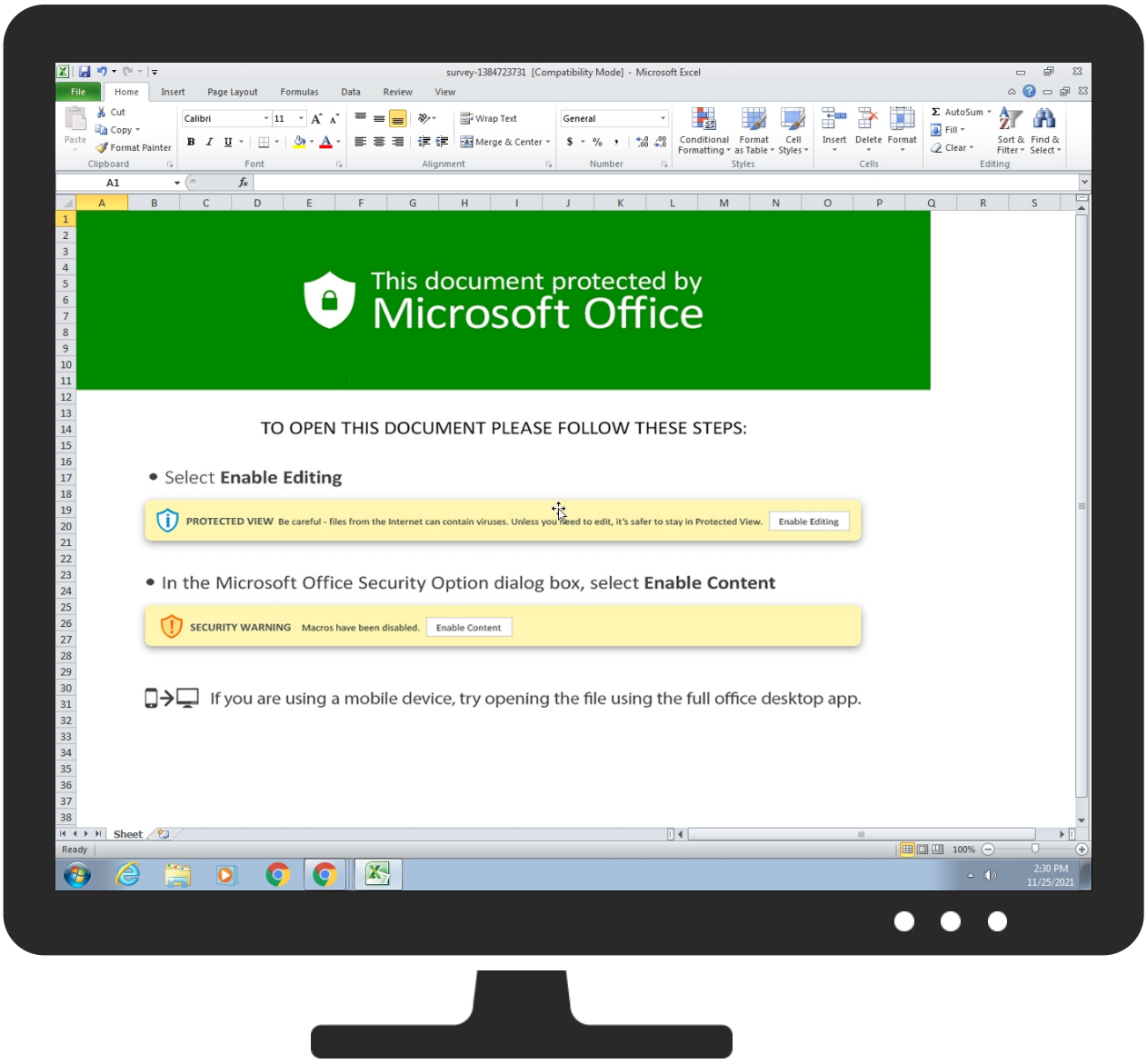


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
klevvrtech.com	0%	Virustotal		Browse
rstebet.co.id	0%	Virustotal		Browse
srkcampus.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://klevvrtech.com/zxywJAC24KJ/ji.html	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://klevvrtech.com/zxywJAC24KJ/ji.html	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://srkcampus.org/OYcMRJbL/ji.html	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	
http://https://rstebet.co.id/fbmKk6n48G/ji.html	2%	Virustotal		Browse
http://https://rstebet.co.id/fbmKk6n48G/ji.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
klevvrtech.com	192.185.79.2	true	false	• 0%, Virustotal, Browse	unknown
rstebet.co.id	103.247.11.218	true	false	• 0%, Virustotal, Browse	unknown
srkcampus.org	192.185.129.7	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://klevvrtech.com/zxywJAC24KJ/ji.html	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://srkcampus.org/OYcMRJbL/ji.html	false	• Avira URL Cloud: safe	unknown
http://https://rstebet.co.id/fbmKk6n48G/ji.html	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.129.7	srkcampus.org	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.79.2	klevvrtech.com	United States		46606	UNIFIEDLAYER-AS-1US	false
103.247.11.218	rstebet.co.id	Indonesia		58487	RUMAHWEB-AS-IDRumahwebIndonesiaCVID	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528587
Start date:	25.11.2021
Start time:	14:30:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	survey-1384723731.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:	mal64.expl.winXLS@7/4@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 application associated with file extension: .xls • 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
14:30:31	API Interceptor	92x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.129.7	survey-1378794827.xls	Get hash	malicious	Browse	
	doc-904268081.xls	Get hash	malicious	Browse	
	doc-904268081.xls	Get hash	malicious	Browse	
	http://ibaylor.psatrans.com/cmlja3lfc293ZWxsQGJheWxvci5lZHU=	Get hash	malicious	Browse	
	http://https://digitek.global/cinetra	Get hash	malicious	Browse	
192.185.79.2	survey-1378794827.xls	Get hash	malicious	Browse	
103.247.11.218	survey-1378794827.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
srkcampus.org	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.129.7
rstebet.co.id	survey-1378794827.xls	Get hash	malicious	Browse	• 103.247.11.218
klevvrtech.com	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.79.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.79.2
	QUOTATION REQUEST DOCUMENTS - GOTO TRADING.exe	Get hash	malicious	Browse	• 162.240.9.164
	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe	Get hash	malicious	Browse	• 192.185.84.191
	Swift Copy TT.doc	Get hash	malicious	Browse	• 50.116.86.94
	8M5ZqXSa28.exe	Get hash	malicious	Browse	• 192.185.129.44
	Change Order - Draw #3 .htm	Get hash	malicious	Browse	• 162.214.66.227

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	Hsbc swift.exe	Get hash	malicious	Browse	• 192.232.249.14
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	microcomputer Official Order.exe	Get hash	malicious	Browse	• 192.185.84.191
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 70.40.220.123
	t 2021.HtML	Get hash	malicious	Browse	• 192.185.129.43
	New Order778880.exe	Get hash	malicious	Browse	• 192.185.167.112
	IyRUJT27dd.exe	Get hash	malicious	Browse	• 192.185.113.96
	LIDlHiVEJQ.exe	Get hash	malicious	Browse	• 162.241.24.173
	bomba.arm	Get hash	malicious	Browse	• 162.144.165.114
	PAYMENT COPY FOR YOUR INFORMATION $76,956.exe	Get hash	malicious	Browse	• 192.185.129.69
	Balance.xls	Get hash	malicious	Browse	• 192.185.113.96
UNIFIEDLAYER-AS-1US	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.79.2
	QUOTATION REQUEST DOCUMENTS - GOTO TRADING.exe	Get hash	malicious	Browse	• 162.240.9.164
	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe	Get hash	malicious	Browse	• 192.185.84.191
	Swift Copy TT.doc	Get hash	malicious	Browse	• 50.116.86.94
	8M5ZqXSa28.exe	Get hash	malicious	Browse	• 192.185.129.44
	Change Order - Draw #3 .htm	Get hash	malicious	Browse	• 162.214.66.227
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	Hsbc swift.exe	Get hash	malicious	Browse	• 192.232.249.14
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	microcomputer Official Order.exe	Get hash	malicious	Browse	• 192.185.84.191
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 70.40.220.123
	t 2021.HtML	Get hash	malicious	Browse	• 192.185.129.43
	New Order778880.exe	Get hash	malicious	Browse	• 192.185.167.112
	IyRUJT27dd.exe	Get hash	malicious	Browse	• 192.185.113.96
	LIDlHiVEJQ.exe	Get hash	malicious	Browse	• 162.241.24.173
	bomba.arm	Get hash	malicious	Browse	• 162.144.165.114
	PAYMENT COPY FOR YOUR INFORMATION $76,956.exe	Get hash	malicious	Browse	• 192.185.129.69
	Balance.xls	Get hash	malicious	Browse	• 192.185.113.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	6docs'pdf.ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	PO201808143_330542IMG_20200710_0008.rtf	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	Order Contract_signed (4NQ39NGAY0GD).ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	new-1834138397.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	new-1179494065.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT-PRIME USD242,357,59.ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	TT-PRIME USD242,357,59.ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	chase.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	private-1915056036.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	private-1910485378.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	SWIFT-MT-103.docx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	Balance.xls	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	original shipping documents.ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	PO 16860.ppam	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	PI-#U00dcRN.Z#U00dcCC.LTD #U015eT.docx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	Clti.xlsx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2
	Vernon.xlsx	Get hash	malicious	Browse	• 192.185.129.7 • 103.247.11.218 • 192.185.79.2

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\91C4.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB 9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF22AC4F44EF579D15.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.309727213192086
Encrypted:	false
SSDEEP:	768:5kmKpb8rGYrMPe3q7Q0XV5xtezEs/68/dgAWuImuZA:5TKpb8rGYrMPe3q7Q0XV5xtezEsi8/d1
MD5:	321156BB89EBDBE9CAEC80FB2A150C47
SHA1:	075C7AF142F023726A0A6246AF33B934C30DB540
SHA-256:	CB714098CBB73CAB579390D9EF687D1B260B30A6303C4BAFB77D8DBCB0E8BC4E
SHA-512:	CA544DDA2062EFB3FE75D55EF85288C989F323BC2935C2574EE3C0CD0C6F10045334A71A99FB723E62949B15B95FDDCA041DC025745C0A13111A5D93DF8620D
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF8E36D078DBA15E72.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\Desktop\survey-1384723731.xls	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
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: Thu Nov 25 10:07:14 2021, Security: 0
Category:	dropped
Size (bytes):	252928
Entropy (8bit):	7.2414057109948615
Encrypted:	false
SSDEEP:	6144:MKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgBcfFw6lxFT7kFWqOSMQ6HujLmH98DUa:kFrlxFTMrvbiFd8Dn
MD5:	55BA35D7D7C154E827124940F26178C7
SHA1:	F51E37DE42F739CCC17E39AD40D121FB1F1E7F88
SHA-256:	37153AA205D42CA882086A9594827B89F8AF82E39A094CE568568AB1E4195ED0
SHA-512:	BAAAA933DBC8C40567067B95A75B8980AFFB809F50238A8A9BC48F7E5F2670C77D1C041FBE462147069CB57188015F3CF3ACB9358DA71FE1C0968C6C497108C
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\survey-1384723731.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\survey-1384723731.xls, Author: Joe Security
Reputation:	low
Preview:	.....>..... .....ZO..... .....\.p....user.8.=. B.....a.....=.....=.....Ve18.....X.@....." .....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.

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: Thu Nov 25 10:07:14 2021, Security: 0
Entropy (8bit):	7.241391186014771
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	survey-1384723731.xls
File size:	252928
MD5:	00bec62d14bc9f8a32948f2c6c512a8f
SHA1:	d2ef80f029f8f035947f1bc6f5929d225374dda4
SHA256:	59d14a53849a19d0dd5ccaf63a85955adbd313c9ec7d92422c0fcdda357b8ce0
SHA512:	34b785ff2f6b964c1285db744a04c62d2b2ef522ced03d0f4896e1a4cc7adf8384167c733b9f2d94ed43bdf6f50ed290e0fe73b7c0942b375d2246a3f65f93dd
SSDEEP:	6144:MKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgBcfFw6lxFT7kFWqOSMQ6HujLmH98DUC:kFrlxFTMrvbiFd8Dr
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "survey-1384723731.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:	2021-11-25 10:07:14
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

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 14:31:11.207514048 CET	192.168.2.22	8.8.8.8	0xa382	Standard query (0)	klevvrtech.com	A (IP address)	IN (0x0001)
Nov 25, 2021 14:31:13.249545097 CET	192.168.2.22	8.8.8.8	0xbd91	Standard query (0)	srkcampus.org	A (IP address)	IN (0x0001)
Nov 25, 2021 14:31:13.907097101 CET	192.168.2.22	8.8.8.8	0xc498	Standard query (0)	rstebet.co.id	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 14:31:11.358360052 CET	8.8.8.8	192.168.2.22	0xa382	No error (0)	klevvrtech.com		192.185.79.2	A (IP address)	IN (0x0001)
Nov 25, 2021 14:31:13.265183926 CET	8.8.8.8	192.168.2.22	0xbd91	No error (0)	srkcampus.org		192.185.129.7	A (IP address)	IN (0x0001)
Nov 25, 2021 14:31:13.944614887 CET	8.8.8.8	192.168.2.22	0xc498	No error (0)	rstebet.co.id		103.247.11.218	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- klevvrtech.com
- srkcampus.org
- rstebet.co.id

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.185.79.2	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-11-25 13:31:11 UTC	0	OUT	GET /zxywJAC24KJ/ji.html 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: klevvrtech.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-11-25 13:31:13 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 13:31:12 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: none Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	192.185.129.7	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-11-25 13:31:13 UTC	0	OUT	GET /OYcMRJbL/ji.html 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: srkcampus.org Connection: Keep-Alive
2021-11-25 13:31:13 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 13:31:13 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 X-Server-Cache: true X-Proxy-Cache: HIT Accept-Ranges: none Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	103.247.11.218	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-11-25 13:31:14 UTC	1	OUT	GET /fbmKk6n48G/ji.html 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: rstebet.co.id Connection: Keep-Alive
2021-11-25 13:31:16 UTC	1	IN	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Thu, 25 Nov 2021 13:31:16 GMT Server: LiteSpeed Alt-Svc: quic=":443"; ma=2592000; v="43,46", h3-Q043=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-25=":443"; ma=2592000, h3-27=":443"; ma=2592000

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 408 Parent PID: 596

General

Start time:	14:30:19
Start date:	25/11/2021
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:	0x13f070000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 2192 Parent PID: 408

General

Start time:	14:30:30
Start date:	25/11/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\besta.ocx
Imagebase:	0xff7e0000
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: 2604 Parent PID: 408

General

Start time:	14:30:31
Start date:	25/11/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\bestb.ocx
Imagebase:	0xff7e0000
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: 1184 Parent PID: 408

General

Start time:	14:30:31
Start date:	25/11/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx
Imagebase:	0xff7e0000
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