ID: 528761
Sample Name: sample2.xls.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:50:04
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

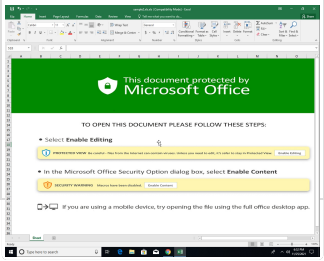
Windows Analysis Report sample2.xls.xls

Overview

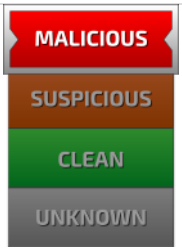
General Information

Sample Name:	sample2.xls.xls
Analysis ID:	528761
MD5:	75c10281f9cae79..
SHA1:	7bd8c6de6d714ff..
SHA256:	53a57594efe3312.
Tags:	vir xlsx
Infos:	

Most interesting Screenshot:



Detection



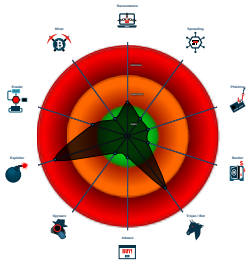
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Performs DNS queries to domains w…
- Office document connecting to susp…
- Potential document exploit detected…
- Yara signature match
- Found a hidden Excel 4.0 Macro she…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5656 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 2336 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4104 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test1.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 7092 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test2.test MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sample2.xls.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x124c8:$s1: Excel • 0x1358c:$s1: Excel • 0x34b5:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
sample2.xls.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
sample2.xls.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\sample2.xls.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x124c8:$s1: Excel • 0x1358c:$s1: Excel • 0x34b5:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
C:\Users\user\Desktop\sample2.xls.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
C:\Users\user\Desktop\sample2.xls.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Command Line Without DLL

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

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Potential document exploit detected (performs DNS queries with low reputation score)

Networking:

Performs DNS queries to domains with low reputation

Office document connecting to suspicious TLD

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:

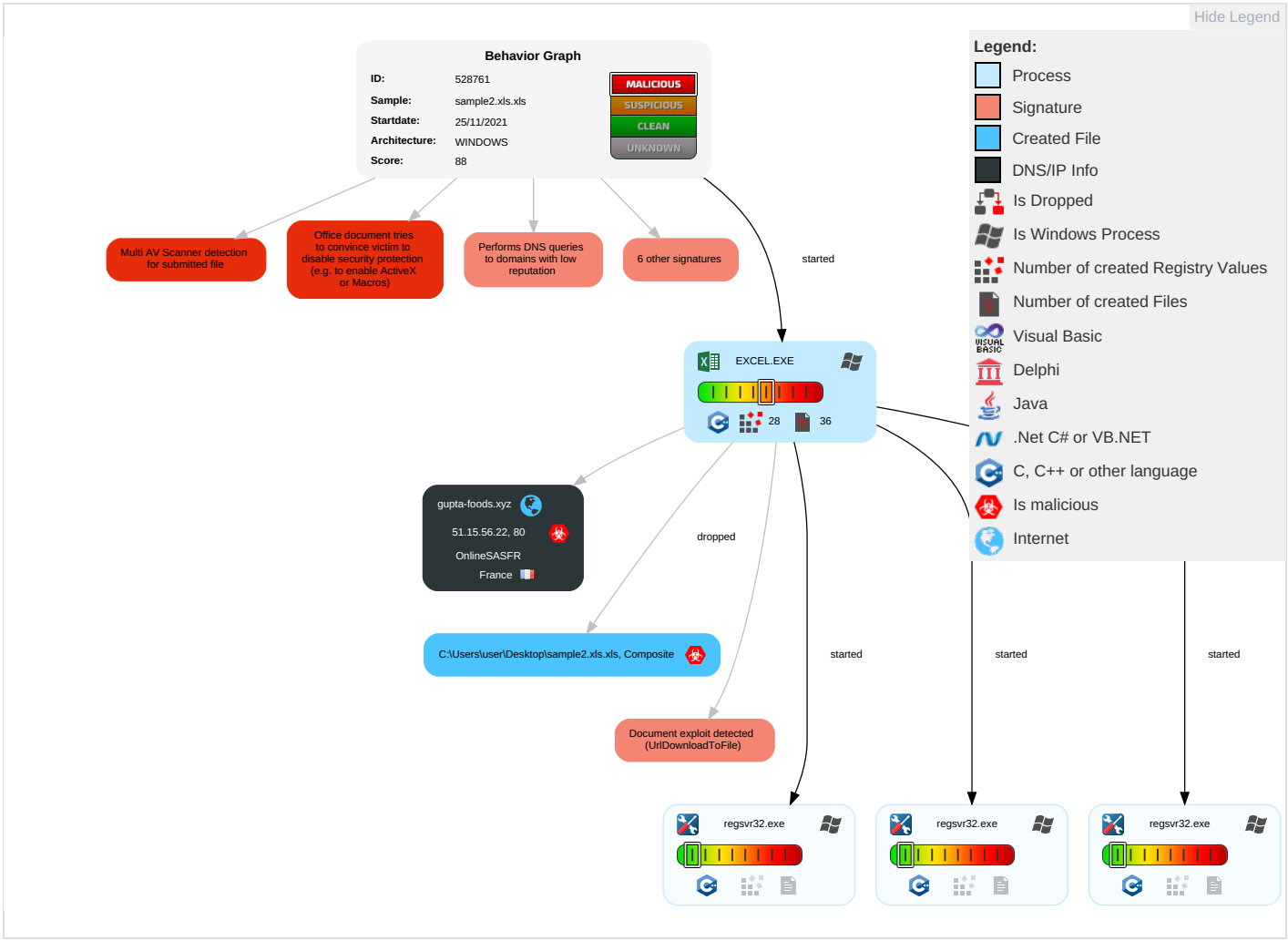
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Ir

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Ir
Valid Accounts	Scripting 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 3 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
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	Protocol Impersonation	SIM Card Swap		C B F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R o

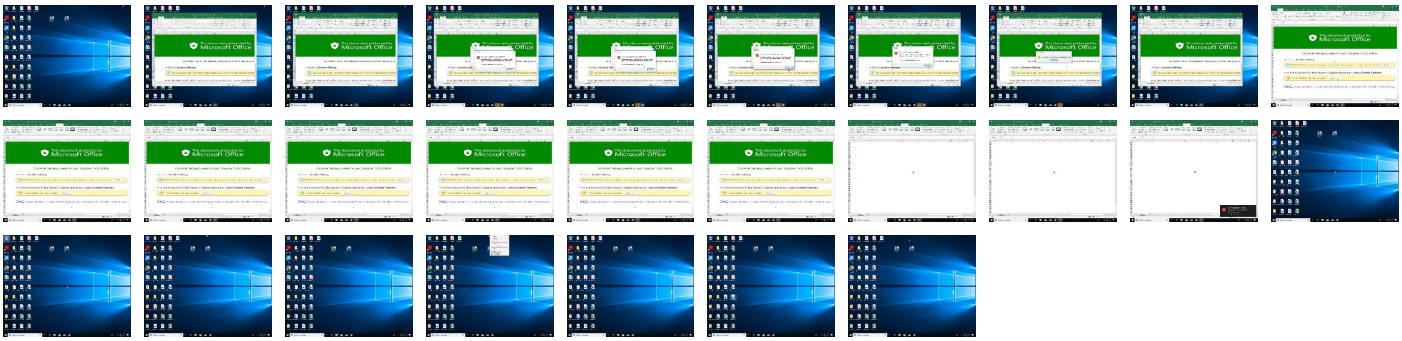
Behavior Graph

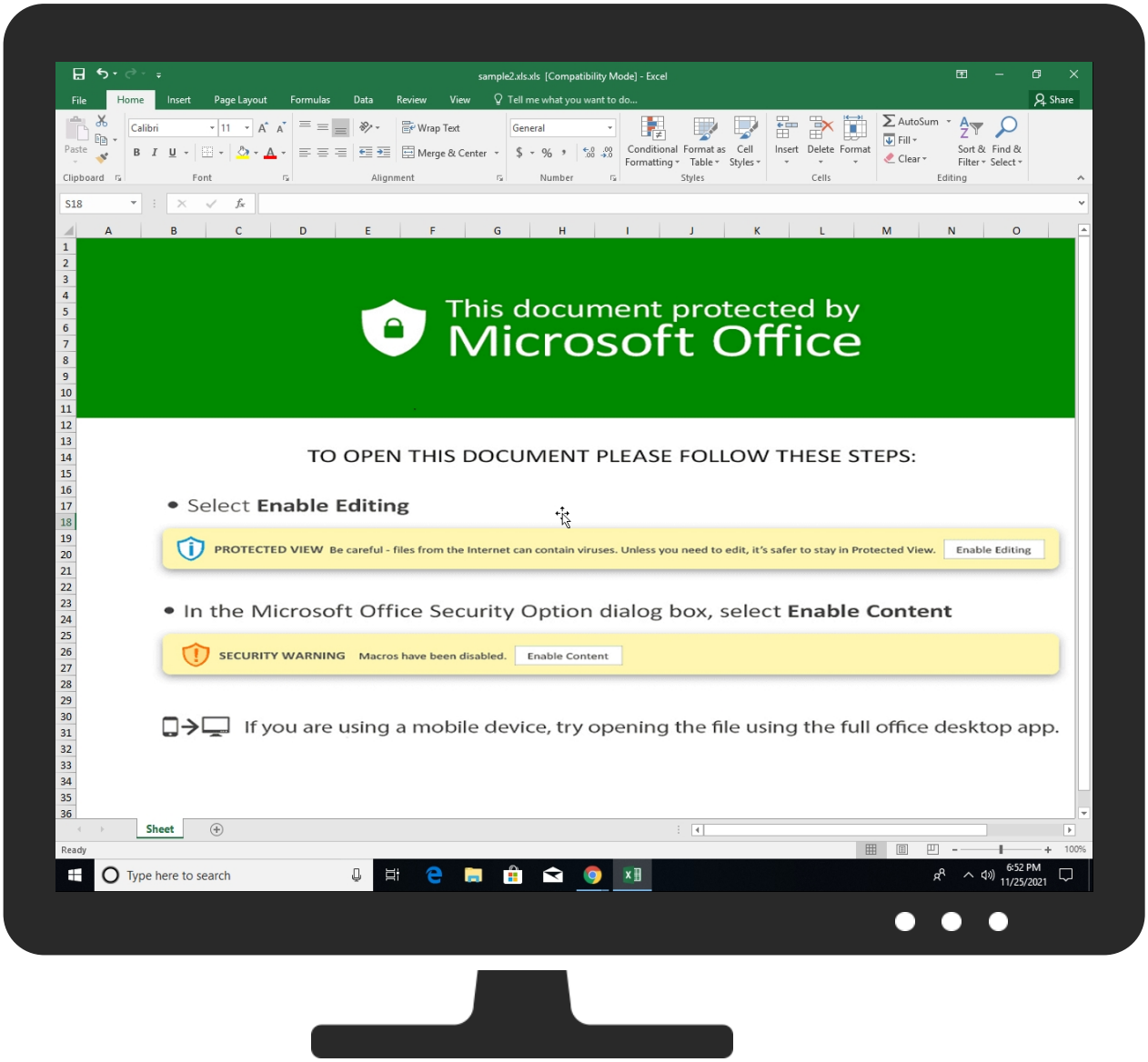


Screenshots

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
sample2.xls.xls	37%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gupta-foods.xyz	51.15.56.22	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.15.56.22	gupta-foods.xyz	France		12876	OnlineSASFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528761
Start date:	25.11.2021
Start time:	18:50:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample2.xls.xls
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	21
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:	mal88.troj.expl.winXLS@7/5@1/1
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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51.15.56.22	sample2.xls.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OnlineSASFR	sample2.xls.xls	Get hash	malicious	Browse	• 51.15.56.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EzCOXP6oxy.dll	Get hash	malicious	Browse	• 195.154.146.35
	IkroV40UrZ.dll	Get hash	malicious	Browse	• 195.154.146.35
	C1Q17Dg4RT.dll	Get hash	malicious	Browse	• 195.154.146.35
	MakbLShaqA.dll	Get hash	malicious	Browse	• 195.154.146.35
	MakbLShaqA.dll	Get hash	malicious	Browse	• 195.154.146.35
	tUJXpPwU27.dll	Get hash	malicious	Browse	• 195.154.146.35
	pYebrdRKvR.dll	Get hash	malicious	Browse	• 195.154.146.35
	pPX9DaPVYj.dll	Get hash	malicious	Browse	• 195.154.146.35
	wUKXjICs5f.dll	Get hash	malicious	Browse	• 195.154.146.35
	cRC6TZG6Wx.dll	Get hash	malicious	Browse	• 195.154.146.35
	qrb6jVwzoe.dll	Get hash	malicious	Browse	• 195.154.146.35
	1711.doc	Get hash	malicious	Browse	• 195.154.146.35
	j9ZfvcmyKN	Get hash	malicious	Browse	• 51.158.220.39
	GQwxmGZFvtg.dll	Get hash	malicious	Browse	• 195.154.146.35
	wNjqkrm8pH.dll	Get hash	malicious	Browse	• 195.154.146.35
	5YO8hZg21O.dll	Get hash	malicious	Browse	• 195.154.146.35
	dUGnMYeP1C.dll	Get hash	malicious	Browse	• 195.154.146.35
	yFAXc9z51V.dll	Get hash	malicious	Browse	• 195.154.146.35
	9fC0as7YLE.dll	Get hash	malicious	Browse	• 195.154.146.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3EDBDB2E-21C4-458B-81F0-642402DEC3FC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140183
Entropy (8bit):	5.357940509156689
Encrypted:	false
SSDEEP:	1536:ecQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:euQ9DQW+zcXfH
MD5:	9496723D7A94F1A139FB3A7C2FC7F7F5
SHA1:	EE0D618C513CE9442E65F78C8E00EB7665CF6F2C
SHA-256:	3D34A159F3D39D5F4C047BFF3C829DA68022B2D8B802EA68F9E8E2BF09B805FC
SHA-512:	C46D798E863E06ABF1224191988C8258894553594B17696CA9DB45563B654F762BADDEAC25A37E600C841C0BFFEABF0D6E2F6AC57408F8617DB0F85E896BB3C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-11-25T17:51:03">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5DA02DEB.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:YmsaITlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5DA02DEB.tmp	
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF4CC8EC7F64F458A9.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.273305538895972
Encrypted:	false
SSDEEP:	768:PPdjpk3hOdsylKlgxopeiBNhZFGzE+cL2kdAJJ6Q470:NNk3hOdsylKlgxopeiBNhZFGzE+cL2ko
MD5:	0223512738657D2EAB010772FCF5EF53
SHA1:	23ECC9BB6DA0227F4DEDE75738AE2E1FF5BB8B52
SHA-256:	4EBDADE7B09BF6CF8824F4564FC018F8BF06EA2C10A15EFEBC263741A2176D4D
SHA-512:	FB51FFB0FECB09C4572D9395D372806AEC4917574317384DBCC38B598AE68371FC92DABEA23D6334D35F0BDB88EF2E53709E8502EF871B44D71B3A2F269F5BE 6
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF620452FF3AABC9C7.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\sample2.xls.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: MacOS, Version 6.11, Code page: -535, Last Saved By: Microsoft Office User, Name of Creating Application: Microsoft Macintosh Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Sun Nov 21 19:57:52 2021, Security: 0
Category:	dropped
Size (bytes):	84480
Entropy (8bit):	6.340434389417097
Encrypted:	false
SSDEEP:	1536:JNk3hOdsylKlgxopeiBNhZFGzE+cL2kdAy91vrVmxJiME2GhdD52lZPFu1AOg0+z:Pk3hOdsylKlgxopeiBNhZFGzE+cL2kdY
MD5:	17EA9CB5F5CA35C7A770EAA508E00E51
SHA1:	89B5243182D096C7237107405B8B585DAF027BF4
SHA-256:	EFFFAEBB90B77CEECB70331FE690CB693A7A1CC57577EA91BA192E8468EE3DE3
SHA-512:	DB550AB75DE0D8A09DD31794FAB8BF2B26403D5120EA8208B5FE5A71BAA897F01AB970C7D58C5F7223E5FF7041D7AE674AEBF72E240755045844A4701E202F3
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: Joe Security • Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: Joe Security

C:\Users\user\Desktop\sample2.xls.xls	
Preview:	.....................>... ....ZO................... ......\.p....prateshft Office User B.....a.........=. ....=........p\D8....... 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..................

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: MacOS, Version 6.11, Code page: -535, Last Saved By: Microsoft Office User, Name of Creating Application : Microsoft Macintosh Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Sun Nov 21 19:57:52 2021, Security: 0
Entropy (8bit):	6.340423482922574
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	sample2.xls.xls
File size:	84481
MD5:	75c10281f9cae799f72d6b949199fd91
SHA1:	7bd8c6de6d714ff5e0b8f450203d24c8dd30495d
SHA256:	53a57594efe3312565fd5415ad3d7066799f831bb685473 7ffaf87fe0119af01
SHA512:	f038bd4f0d0d6108502a761de35d10cb53b7351c18b744 4c9b247bbf10fdc8962fe516f90c1a05a7583731711dcd9 8b46a3667a3e9d9f79a48d035fc0e1ba49
SSDEEP:	1536:oNk3hOdsylKlgxopeiBNhZFGzE+cL2kdAy91vrVm xJiME2GhdD52lZPFu1AOg0+d:wk3hOdsylKlgxopeiBNh ZFGzE+cL2kd0
File Content Preview:	........................>.. ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sample2.xls.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Macintosh 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:	-535
Author:	
Last Saved By:	Microsoft Office User
Create Time:	2015-06-05 18:19:34

Summary

Last Saved Time:	2021-11-21 19:57:52
Creating Application:	Microsoft Macintosh Excel
Security:	0

Document Summary

Document Code Page:	10000
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 18:51:08.404145002 CET	192.168.2.3	8.8.8.8	0x67de	Standard query (0)	gupta-foods.xyz	A (IP address)	IN (0x0001)

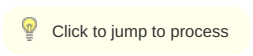
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:51:08.458050966 CET	8.8.8.8	192.168.2.3	0x67de	No error (0)	gupta-foods.xyz		51.15.56.22	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 5656 Parent PID: 744

General

Start time:	18:51:00
Start date:	25/11/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x8e0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 2336 Parent PID: 5656

General

Start time:	18:51:29
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\test.test
Imagebase:	0xa00000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 4104 Parent PID: 5656

General

Start time:	18:51:29
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\test1.test
Imagebase:	0xa00000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B

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: 7092 Parent PID: 5656

General

Start time:	18:51:30
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\test2.test
Imagebase:	0xa00000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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