ID: 431855
Sample Name: audit-367497006.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:16:15
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

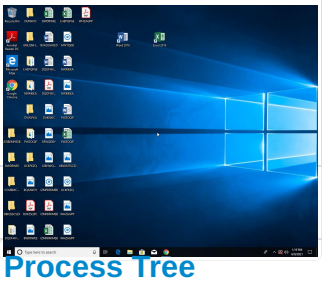
Analysis Report audit-367497006.xlsb

Overview

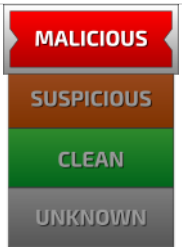
General Information

Sample Name:	audit-367497006.xlsb
Analysis ID:	431855
MD5:	6a44858ca2fe28f..
SHA1:	e793cbf64ad364c..
SHA256:	49558300c4315c..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection



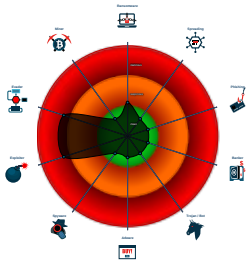
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5980 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 4112 cmdline: regsvr32 -s ..\werty1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 660 cmdline: regsvr32 -s ..\werty2.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

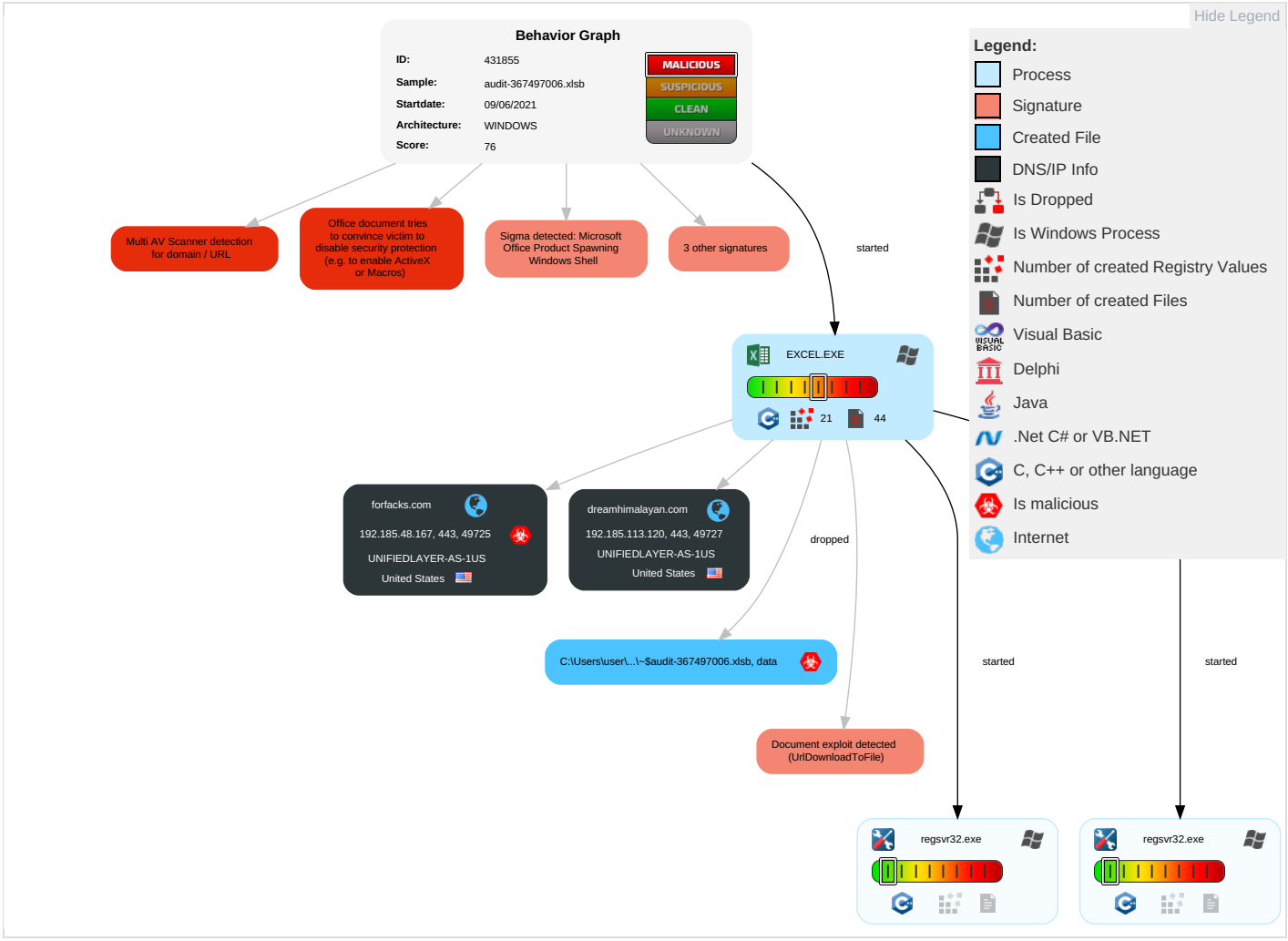
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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
Valid Accounts	Scripting 2	DLL Side-Loading 1	Process Injection 1	Regsvr32 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

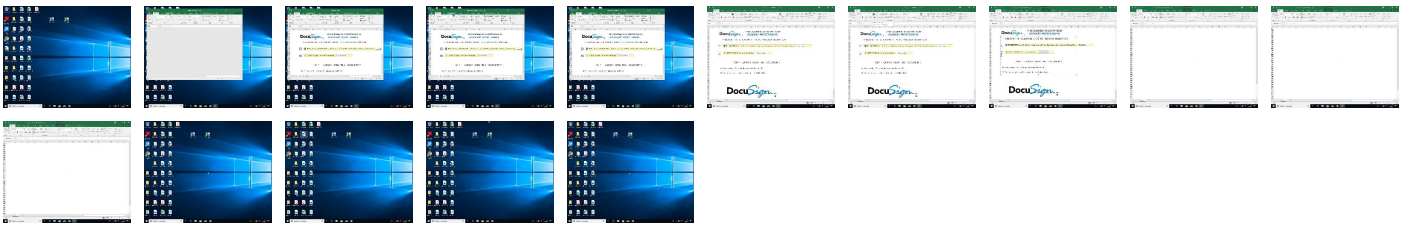
Behavior Graph



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
dreamhimalayan.com	0%	Virustotal		Browse
forfacks.com	6%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dreamhimalayan.com	192.185.113.120	true	false	• 0%, Virustotal, Browse	unknown
forfacks.com	192.185.48.167	true	true	• 6%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.48.167	forfacks.com	United States		46606	UNIFIEDLAYER-AS-1US	true
192.185.113.120	dreamhimalayan.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431855
Start date:	09.06.2021
Start time:	13:16:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	audit-367497006.xlsb
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
Number of analysed new started processes analysed:	3
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:	mal76.expl.evad.winXLSB@5/9@2/2
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: .xlsb • 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
192.185.113.120	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• www.guepard-marine.com/ivay/?PbvpO8=7c4TMZ8HJw/eFJUVC4Rd5gN+5dnR2WOvXzuZPR1ukaHcCIIPr6KkFYNadeo0+7aaqJva+Q==&-Zp=fxoDxR_8sz1ds
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• www.guepard-marine.com/ivay/?oPnpM4=7c4TMZ8CJ3/aFZYZA4Rd5gN+5dnR2WOvXz2JTSpvg6HdC5kJsqboTc1Ye7Ei6rephKyq&Lh0l=ZTdp62D8T

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	analysis-31947858.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	research-531942606.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	• 192.254.185.244
	research-121105165.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-76934760.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-1960540844.xlsx	Get hash	malicious	Browse	• 192.185.33.8
	fm8m5vuj2w.exe	Get hash	malicious	Browse	• 192.185.26.241
	research-1110827633.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	swift_08_06_21.exe	Get hash	malicious	Browse	• 162.241.61.204
	INVOICES,PDF.exe	Get hash	malicious	Browse	• 192.254.224.94
	Outstanding_Payments.exe	Get hash	malicious	Browse	• 192.185.129.69
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 192.185.107.121
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 192.185.145.162
	SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe	Get hash	malicious	Browse	• 192.185.113.219
	SecuriteInfo.com.__vbaHresultCheckObj.9138.exe	Get hash	malicious	Browse	• 192.185.113.219
	MLJ.exe	Get hash	malicious	Browse	• 192.185.113.219
	LEMOH.exe	Get hash	malicious	Browse	• 162.241.219.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	03062021.exe	Get hash	malicious	Browse	• 162.241.253.69
	Shipment documents.exe	Get hash	malicious	Browse	• 192.185.190.186
UNIFIEDLAYER-AS-1US	analysis-31947858.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 108.167.156.223
	research-531942606.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	• 192.254.185.244
	research-121105165.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-76934760.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	research-1960540844.xlsx	Get hash	malicious	Browse	• 192.185.33.8
	fm8m5vuj2w.exe	Get hash	malicious	Browse	• 192.185.26.241
	research-1110827633.xlsb	Get hash	malicious	Browse	• 192.185.33.8
	swift_08_06_21.exe	Get hash	malicious	Browse	• 162.241.61.204
	INVOICES,PDF.exe	Get hash	malicious	Browse	• 192.254.224.94
	Outstanding_Payments.exe	Get hash	malicious	Browse	• 192.185.129.69
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 192.185.107.121
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 192.185.145.162
	SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe	Get hash	malicious	Browse	• 192.185.113.219
	SecuriteInfo.com.__vbaHresultCheckObj.9138.exe	Get hash	malicious	Browse	• 192.185.113.219
	MLJ.exe	Get hash	malicious	Browse	• 192.185.113.219
	LEMOH.exe	Get hash	malicious	Browse	• 162.241.219.209
	03062021.exe	Get hash	malicious	Browse	• 162.241.253.69
	Shipment documents.exe	Get hash	malicious	Browse	• 192.185.190.186

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Bills Pending Approval.html	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	GDrVYvtzuO.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	9E7YOr0kp1.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	aKdhpWlFPg.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	vSYEHJjK1G.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	FaceCheck - Installer.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	analysis-31947858.xlsb	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	Julie.randall Completed REFERRAL AGREEMENT 60926.html	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	x1Q123VhUa.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	Snc3sPQ2yl.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	nU8kVKVAc8.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	research-531942606.xlsb	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	New order_doc.exe	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	research-121105165.xlsb	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120
	New order_doc.lzh	Get hash	malicious	Browse	• 192.185.48.167 • 192.185.113.120

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2A108F49.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 246 x 108, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	10270
Entropy (8bit):	7.975714699744477
Encrypted:	false
SSDEEP:	192:3sXvKLMbye/PEXiKTUgCto9h4F6NwfU6vGDpdYNbcQZgkbd4cgc:3iLh/gJ59CDfU6LocbGK
MD5:	9C4F09E387EA7B36C8149EA7C5F8876E
SHA1:	FF83384288EB89964C3872367E43F25FAFF007CC
SHA-256:	A51C1D65092272DAEB2541D64A10539F0D04BC2F51B281C7A3296500CFCA56DE
SHA-512:	0FDDE22CFDDE8BB1C04842D2810D0FD6D42192594E0D6120DE401B08B7E2CFFB5333792BC748E93CD70FA14734CC7D950620CB977DDBBDB52D92BDA8F3552F8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....l.....sRGB.....pHYs.....+....'.IDATx^.].|.U...%...J."....H.&Ui.....E.....D.7....U.i..FH#=.....3..$K....'{3....7.....0.H.....H..03..,....8.q.....'@\. ..S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8..... .`..) @...X...q..>N...>.....q.....'@\...S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8...l..m.i'Sj.W.i.S.TJ....D.D._%...] ..i.;J..b..T.).lk.L6..L.mN....!*..\..'{$.o._b..h....t"@.?...y...d..h..|..B9D..CJD..t."....bR"....I)H....z.....>|.....E.x..r....J.U..[...p:D....XF.....A...E.....b..C...C..C.....=.Z..$.=../....Y ..x5CY.0l..,~.W. .?.....;...$.'....<.H.2...z..6(.E.....kw8w^.\~...".C,gl&.m..J2.).HI.....b.r...'.....r.H...P....'...A.^.q..j).cZ.^1~.|.....dv^.^v..X..v..6/^.$rR. iK..H.Uu.Pvk....U.....'.Fd..Z .]mu*1.Zb.\b...N..P..&tr;.W....J.K(@.^A..R.S.[~.v.R.YO...0-...2..h."..............7..Ng...R...e.&..@..t..N...{5...W.x./#.%..}t...F8-..M1..(4b1....&.....)B...6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5C50E7CA.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 521 x 246, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	32996
Entropy (8bit):	7.975478139053759
Encrypted:	false
SSDEEP:	768:N4k48AnTViUidx37OODgvnrxtxAudMN1VTRVHdB4K7K:NE8m+L37OOwrCXN1VTR1PK
MD5:	4E69B72B0CE87CC7EE30AA1A062147FE
SHA1:	09B0AA5414E08756E0AE53E1BE5C70DB4DEAF2E8
SHA-256:	77A1F749389CBF771D5197FF0FF17113FCA1D91989ADCADF2852876A6CC14988
SHA-512:	6246AF2137E773F7719033AFE75F0B00FF3A4B5543DBA53737FC8D33EE42478E3D8A5CF166E9EFD2F54A2F3E0D62417BDDC1CB824642305B59AB1229313D2D7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5C50E7CA.png	
Preview:	.PNG.....IHDR.....[.J....sRGB.....pHYs.....+.....IDATx^.].`.....{%.$..A...R.P@z....O...S.<;.VT.REA.(...I...{.....m...]..r./.....~.|]h.Z....P.(.....E."@...P.(.v.P.@..E."@. ...#@y.....E."@y.....E."...*78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...)..... !@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P ..!@y.3.....E....."@...8C...g...)......!@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3 ..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...)......!@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8F304143.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9F7E393F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 490 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	18547
Entropy (8bit):	7.9850486438978985
Encrypted:	false
SSDEEP:	384:kBCIQCloAwCZDy0xOTn6/g6l4NpWfw9nHk6Ka01f7Y/H:kBCIQpAwODPMT6/gfOUKN70
MD5:	ED31C7053D581EDC4C98D222CE02EDEF
SHA1:	6BA7A49CC6FF8FE00E9C5BC75F48AB7E679536DD
SHA-256:	0FCF61397154DF01CFAECA362BD643D88AAD5FEDD07B52DC8A921CC0D7236534
SHA-512:	929BF13F2A050B33D0EABDAC97CAAFDDE612AD521027FEE4DD51E28A3CF61198D6C045E00AB85223C73D74D18BB4EAA1681C7AFA917946DC08A3C75FB2AB4 935
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....l{.....sRGB.....pHYs.....+....H.IDATx^...U....."x....U...."...Tc.{...M1M..In....TATb4F,`oD..Q..3.....g.3..Lr.D....a8....~.z....Z...yyF..9...:.H .Q2..)/L.....Q.}....(J.,...w2>R.$..G2..m>..|...0.M.g.Xnjj...P.v..x....S.....B..p.=.Lz.^..Wi..2U.V'.a..*DE.'..rT.z....#.;..]....[?.C...o.m`]..m][;.:<..]F.9..u..Q]c.Ue.9....(.F.Z.~s..Q:..B.. .)..LZ.TTo..P.gc.l.'.X.}..H....Q.h\|....L..rcd.2dN..co..5.....w.U.4..}.....{.Q.....D2.J.z~..:Y3,.H..(#.J.Q.....N.._7....w.....].2w.6...._....u.....9-.7.f9...E9...p.A..f....=....Bqu....A .u.JG>b"...%..0..W.H=...G#.DR.....P.\|FD).NJ....)>.;...M...T*.dW..t:[.xT..M.\|S...O..."M.4u7.uS...]4..R.vK....*).ZK.. J.=.9C.].kr..ES..6..f.(.....N':..t..^.S....kn[s.#..(.....m.....~....6>.... :u.J.mO.....%D...Q...6%....!.....H.....v..^%....$.._.V.....[o5.H8.....n.~M.z.RL.0p:.iC.k.1..$.....3[....mS5.....E...2.&...k]...A.....K.8...5..O.@7.[-.F4*7...i....in...y....A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BA0F5CB6.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 934 x 29, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	42557
Entropy (8bit):	**7.992800895943226**
Encrypted:	**true**
SSDEEP:	768:Pfsq4UmepRdblCFcXhw9KnRTRews6xD0FvBlwAS1A8x7BcS0OvD230:PR3ZblCF28KRsws6CFv0AYx7Bl3b230
MD5:	B1F262A694930ADB699FA94E3394887F
SHA1:	9C9B66D3A3F09AECA45DB94304CDD6FB3C5BD4C9
SHA-256:	9C99EC61392B9022A38C1354124360147E8185065095BD2EC92B1416CF9F4B68
SHA-512:	1CA7E6750178B88EC3AA7A0B83348EA389E26C27E0D7E919D807BE470714E5B4F04ACEB69D391F0498D4E465E6620E9449CA2F40755B5CE8196E683502EBF5F4
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....6.....sRGB.....pHYs.....+.....IDATx^....dU....S.:ON.0.0....s0 .....$..%#HR.T.....$..0C...Su...[.TM..{.....C.S}..^{.....].^..ZX.Wb.W....X!..A.P... .0..u...X.V.3.....z..tiO{GW..?...A.....ca2Y.... ...cAX..zZ..2M.$..g.O.e..r?z&.....*....*.=..Z.A.....a.Z..ka<..N.R.c...../.[..j.^...Nk.(..y.,..z"...R..Z+..D1Q....z....0..u~. .jU_.b.Z.V....:.5:.(.....-...A2.O.{..p.j..].<.....0..0..+....E...^...z....#..j.d...X._..1..M.5..O.^..".I....G....U1.....X.6.Z.\.&..h..m*..T..xH.j..3<$.H...a..n....}t.A.jT.6G.h@..<.x..x...cb.. ....C..{.D.'QW<.o~..?.....4F_..B..h.\...y8..)....j.Z.d..#P..P..O.....(.0...f....B_z>.E .w../..(...'.Fw..yT..G..)...b9..g.AA`.a..v.zfY.F....._r.i.d.`....Q.g.m"..\..&.t.X.q1}.$.S....2..~...d."..1.. (.0.F....t...i..@f.. ...(..8..q.....I.....ad.....z%....;...y.O...X<Q..X.....B..H.....<).....4.&9.4.....1.h..#B.....g.....bO.59.A..M.....J..vX3*5..X....(G.A.u...8.. .{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DEFF0268.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.IR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Temp\05A40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	157782
Entropy (8bit):	7.964514317513524
Encrypted:	false
SSDEEP:	3072:LdlQ9VlUBWA6CFvA7brCxAVIKDXv/V1REyNEsAnexVymd1xXPw2N:Lw3liWA6FiYDXvNfzTYexVyWxfB
MD5:	1F2A5A98E12F173129B088345FFF61F3
SHA1:	C817375FF59A4588B3E061EB1D977B6ACA6761A0
SHA-256:	80C5336B8456DE56D4346B3E990CF7108C3F7B4C8FA0E5C19B106EEA740EBBEF
SHA-512:	638D7E4111976BEF9EAB836BF188A2E01299640D9617FA611D9537A264F0970083C5A14431EA0FC2EB0814B564472E92D018A0B4C8F9CFD7EF57BE8AF8164B51
Malicious:	false
Preview:	.U.N.0.}G.....J\@Z!....w.`?....U..1..=c7..JK)...'s.3.x|...z.....7#V..^i....u}.*L.)a...-.....n..+.v.>.p.9.....p...hE.... .\t.OF._\z...:e.6._.L.T]-hy.d...~...T-.!.-E"....w$.....%..C....H.4!jb..... o...{.m..7gD0.....2K)..?...r.c.....T7".?.[|a.....f;H6.b....).5V.....Y.....?A.v.l._.....Qt.B....b.....c..t.....\..g..a'.....6..].k..:T..Y.....}...K3.&..4.#....D..u .I.z.m..kF.....@m...<.. .....PK.....!.[:.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$audit-367497006.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF

C:\Users\user\Desktop\~$audit-367497006.xlsb	
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.957827832827454
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	audit-367497006.xlsb
File size:	157733
MD5:	6a44858ca2fe28f5e2c4eed2c5a360e4
SHA1:	e793cbf64ad364c93e3a673a090977a3434cb6d9
SHA256:	49558300c4315c8c53216a8c17e32ff87ca4be34547ab064de7d872d429bb3f3
SHA512:	c1f3e1eeb05ef311c4a65fa80914d0e18e42becb3ca6e956fd165c4013ec82eacd844f7cdc79d73f61b958ac6e53e2dcc1296c830d4c03ab5fbb54b4bfcfe593
SSDEEP:	3072:VzjTemXbxVymd1xXPMU9VlUBWA6CFvA7bRCxAVIKxS6:RTecbxVyWxfMU3liWA6FsYn
File Content Preview:	PK.....!...k....."....[Content_Types].xml ...(.....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "audit-367497006.xlsb"

Indicators

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

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
Jun 9, 2021 13:17:06.734746933 CEST	192.168.2.4	8.8.8.8	0x530	Standard query (0)	forfacks.com	A (IP address)	IN (0x0001)
Jun 9, 2021 13:17:08.120975971 CEST	192.168.2.4	8.8.8.8	0xc26d	Standard query (0)	dreamhimalayan.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 13:17:06.912420988 CEST	8.8.8.8	192.168.2.4	0x530	No error (0)	forfacks.com		192.185.48.167	A (IP address)	IN (0x0001)
Jun 9, 2021 13:17:08.164104939 CEST	8.8.8.8	192.168.2.4	0xc26d	No error (0)	dreamhimalayan.com		192.185.113.120	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 9, 2021 13:17:07.277209044 CEST	192.185.48.167	443	192.168.2.4	49725	CN=*.forfacks.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 16 07:28:43 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 14 07:28:43 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 9, 2021 13:17:08.491446018 CEST	192.185.113.120	443	192.168.2.4	49727	CN=*.dreamhimalayan.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 16 02:04:50 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 14 02:04:50 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5980 Parent PID: 800

General

Start time:	13:17:01
Start date:	09/06/2021
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:	0x1010000
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

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 4112 Parent PID: 5980

General

Start time:	13:17:08
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\werty1.dll
Imagebase:	0x2e0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 660 Parent PID: 5980

General

Start time:	13:17:09
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\werty2.dll
Imagebase:	0x2e0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis