ID: 339446
Sample Name: sample1.bin
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 03:59:37
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

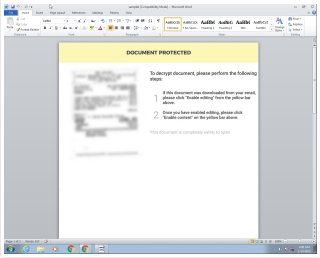
Analysis Report sample1.bin

Overview

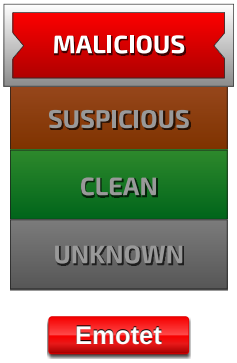
General Information

Sample Name:	sample1.bin (renamed file extension from bin to doc)
Analysis ID:	339446
MD5:	7dbd8ecfada1d39.
SHA1:	0d21e2742204d1..
SHA256:	dc40e48d2eb0e5..

Most interesting Screenshot:



Detection

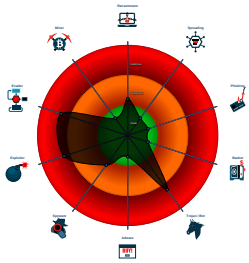


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Snort IDS alert for network traffic (e…
- Yara detected Emotet
- Creates and opens a fake document…
- Creates processes via WMI
- Document contains an embedded VB…
- Drops PE files to the user root direc…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2264 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- certutil.exe (PID: 2440 cmdline: Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
- svchost.exe (PID: 2348 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- tmp_e473b4.exe (PID: 1772 cmdline: C:\Users\user\AppData\Local\Temp/tmp_e473b4.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
  - auditpolmsg.exe (PID: 1688 cmdline: C:\Windows\SysWOW64\srclient\auditpolmsg.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
    - wcnwiz.exe (PID: 2064 cmdline: C:\Windows\SysWOW64\mfc110\wcnwiz.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
      - SampleRes.exe (PID: 2004 cmdline: C:\Windows\SysWOW64\capiprovider\SampleRes.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
        - NlsData0414.exe (PID: 2364 cmdline: C:\Windows\SysWOW64\RMActivate_ssp_isv\NlsData0414.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
          - mfc140.exe (PID: 1664 cmdline: C:\Windows\SysWOW64\KBDNO\mfc140.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
            - ieframe.exe (PID: 1236 cmdline: C:\Windows\SysWOW64\advapi32\ieframe.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
              - cryptdll.exe (PID: 2728 cmdline: C:\Windows\SysWOW64\nshipsec\cryptdll.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
                - wlanui.exe (PID: 2832 cmdline: C:\Windows\SysWOW64\DShowRdpFilter\wlanui.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2256698017.00000000003F1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000003.2262096055.0000000000548000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2279698396.00000000003E1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000A.00000003.2266631097.0000000000578000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000003.2252976219.0000000000588000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

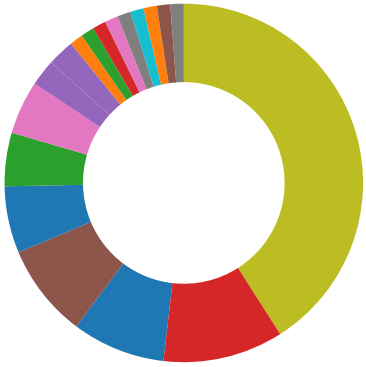
Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.mfc140.exe.3e0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.SampleRes.exe.7b0000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.ieframe.exe.320000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
14.2.cryptdll.exe.620000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
15.2.wlanui.exe.480000.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

E-Banking Fraud:

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro with suspicious strings

Persistence and Installation Behavior:

Creates processes via WMI

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Creates and opens a fake document (probably a fake document to hide exploiting)

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information:

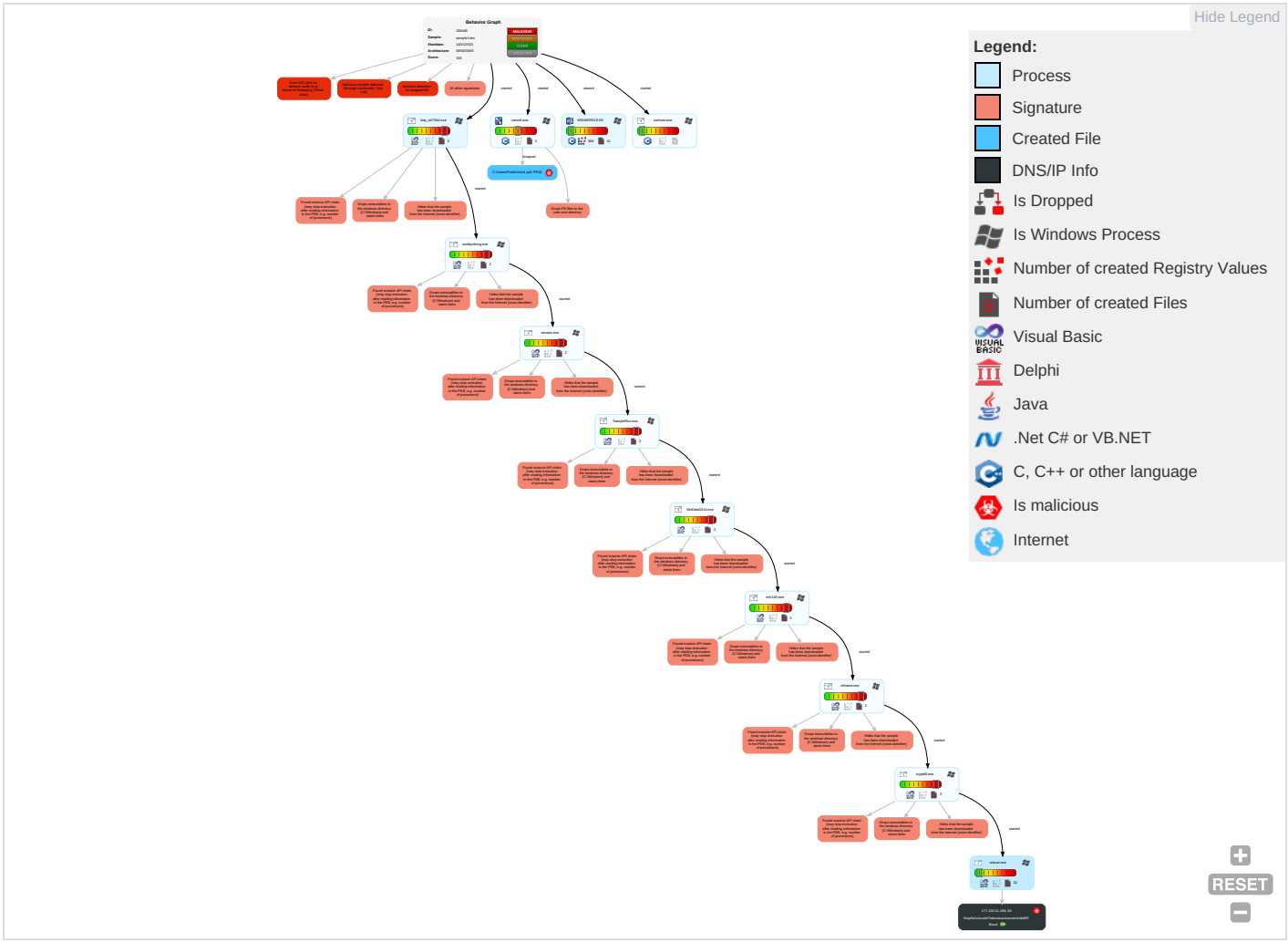
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Windows Management Instrumentation 1 1	Windows Service 1 2	Windows Service 1 2	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Ea Ins Ne Co
Default Accounts	Scripting 1 2	Boot or Logon Initialization Scripts	Process Injection 1 1	Scripting 1 2	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2	Ex Re Ca
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Ex Tra Lo
Local Accounts	Exploitation for Client Execution 1 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 1 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SI Sw
Cloud Accounts	Command and Scripting Interpreter 1	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Service Execution 1 1	Rc.common	Rc.common	Masquerading 2 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dc Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

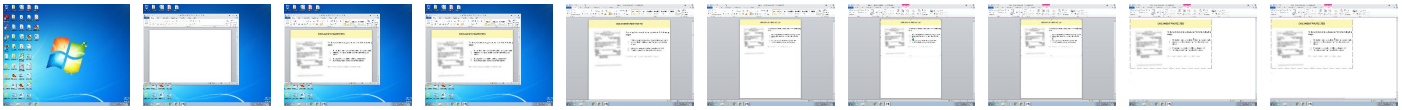
Behavior Graph

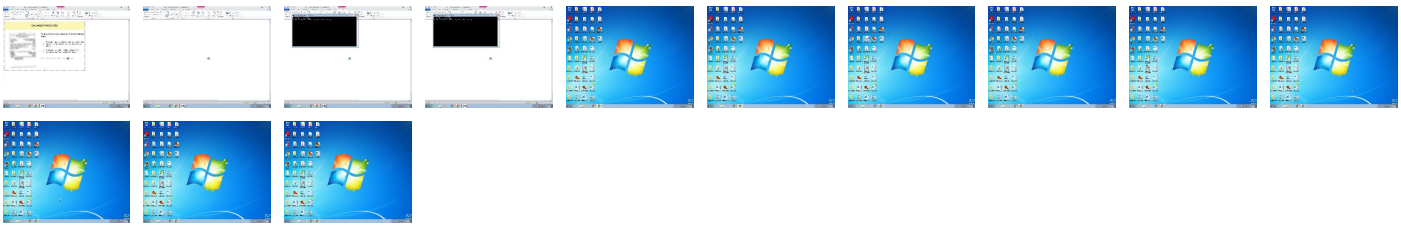


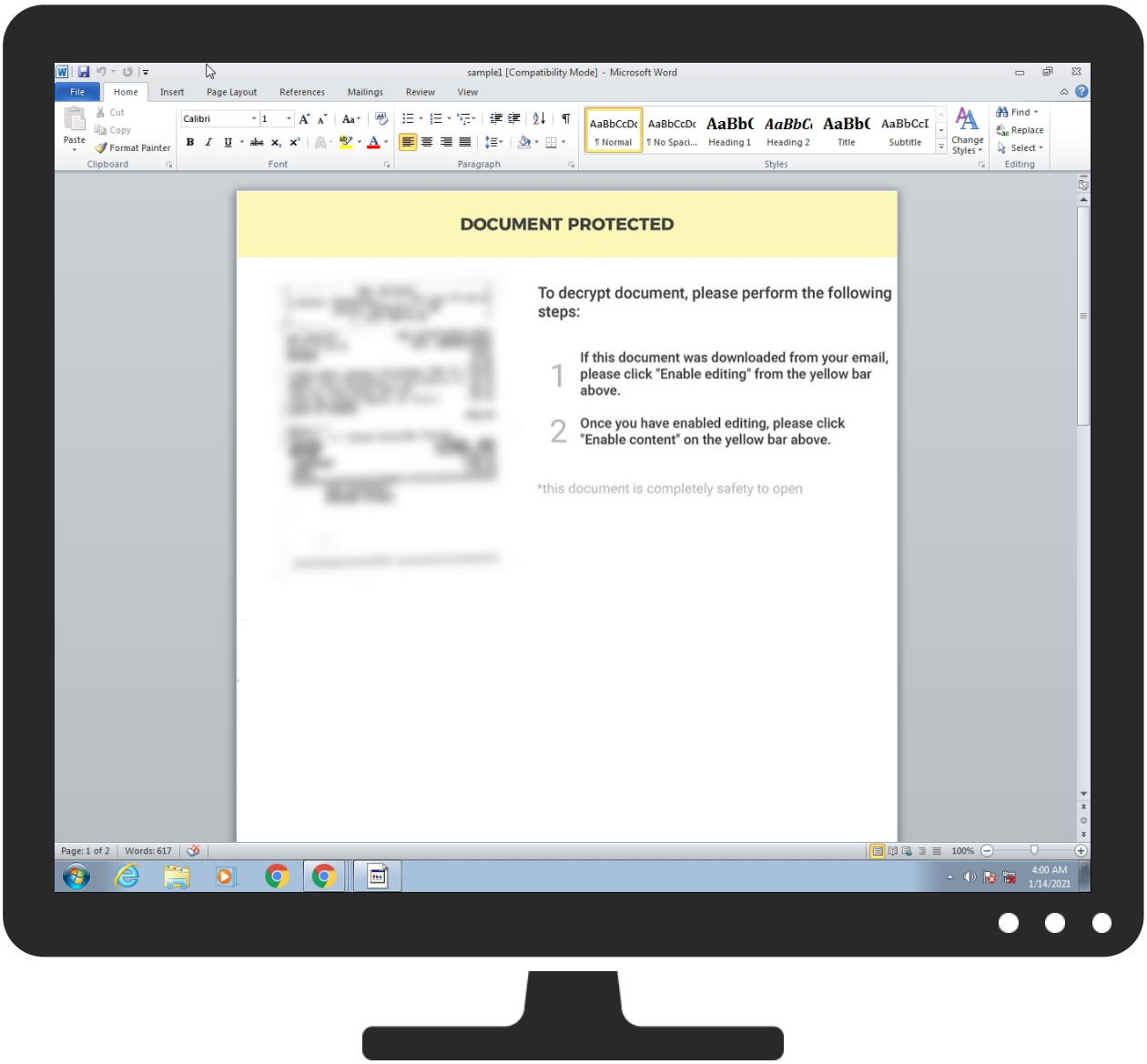
Screenshots

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
sample1.doc	62%	Virustotal		Browse
sample1.doc	46%	Metadefender		Browse
sample1.doc	72%	ReversingLabs	Document-Word.Trojan.Valyria	
sample1.doc	100%	Avira	HEUR/Macro.Downloader.MRYT.Gen	
sample1.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Ksh1.pdf	100%	Avira	TR/Casdet.xqfgu	
C:\Users\Public\Ksh1.pdf	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\Public\Ksh1.pdf	41%	Metadefender		Browse
C:\Users\Public\Ksh1.pdf	64%	ReversingLabs	Win32.Trojan.Malrep	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.ieframe.exe.320000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.1.wcnwiz.exe.39b0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.1.cryptdll.exe.3ab0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.1.tmp_e473b4.exe.3a20000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.mfc140.exe.3e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.1.ieframe.exe.39f0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.0.wcnwiz.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
10.2.SampleRes.exe.7b0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.tmp_e473b4.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
10.1.SampleRes.exe.39e0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.2.wlanui.exe.480000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.cryptdll.exe.620000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.wlanui.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
13.0.ieframe.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
8.0.auditpolmsg.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
7.1.tmp_e473b4.exe.3a20000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.cryptdll.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
12.1.mfc140.exe.3980000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.mfc140.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
8.1.auditpolmsg.exe.39b0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.tmp_e473b4.exe.3f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.NlsData0414.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
10.0.SampleRes.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
11.1.NlsData0414.exe.39c0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.NlsData0414.exe.2b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.wcnwiz.exe.3b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.auditpolmsg.exe.360000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://pornthash.mobi/videos/tayna_tung	0%	Avira URL Cloud	safe	
http://https://pornthash.mobi/videos/tayna_tung%temp%/tmp_e473b4.exex	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

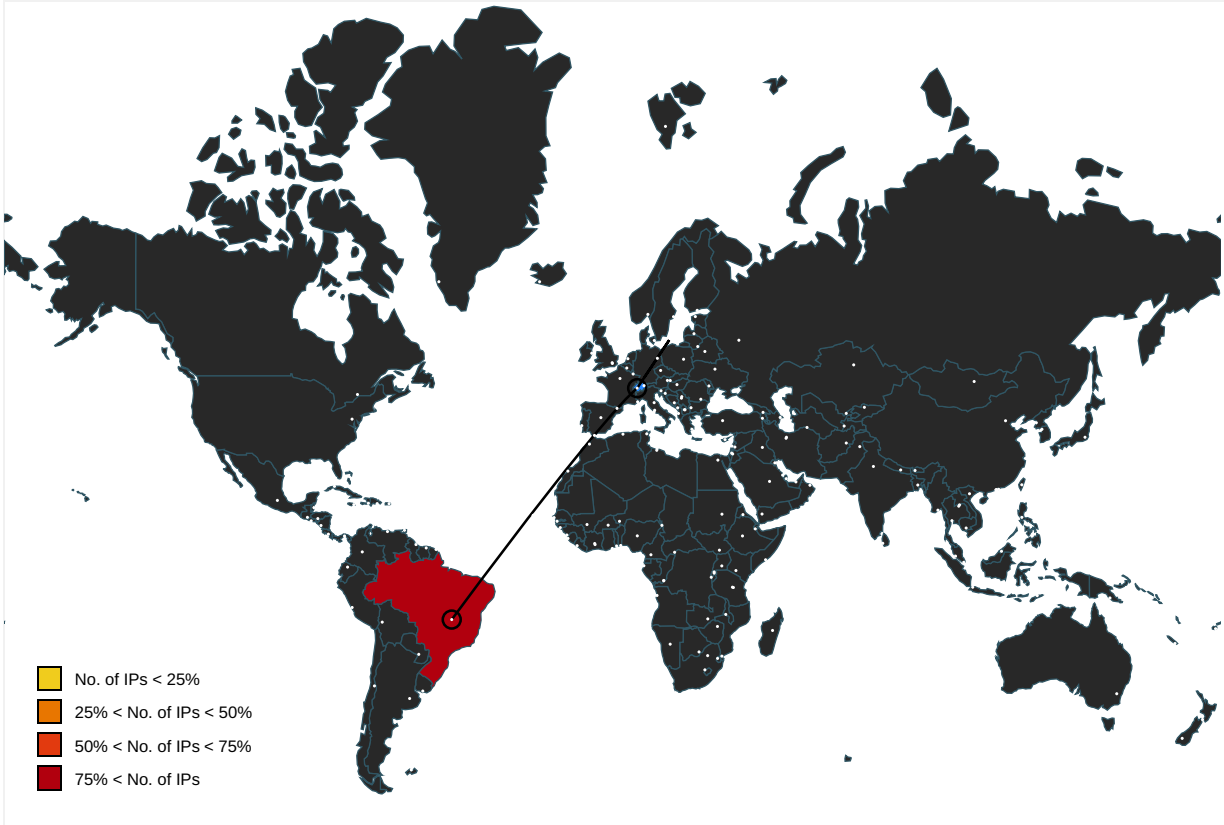
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	certutil.exe, 00000001.0000000 2.2223417988.00000000022A0000. 00000002.00000001.sdmp, tmp_e4 73b4.exe, 00000007.00000002.22 58709906.00000000030D0000.0000 0002.00000001.sdmp, auditpolmsg.exe, 00000008.00000002.2265231662.0000 000002F30000.00000002.00000001 .sdmp, wcnwiz.exe, 00000009.00 000002.2269936188.000000000306 0000.00000002.00000001.sdmp, S ampleRes.exe, 0000000A.0000000 2.2273974582.0000000002F20000. 00000002.00000001.sdmp, NlsDat a0414.exe, 0000000B.00000002.2 278988967.0000000003000000.000 00002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://pornthash.mobi/videos/tayna_tung	certutil.exe, 00000001.0000000 2.2223923762.0000000002770000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	certutil.exe, 00000001.0000000 2.2223417988.00000000022A0000. 00000002.00000001.sdmp, tmp_e4 73b4.exe, 00000007.00000002.22 58709906.00000000030D0000.0000 0002.00000001.sdmp, auditpolmsg.exe, 00000008.00000002.2265231662.0000 000002F30000.00000002.00000001 .sdmp, wcnwiz.exe, 00000009.00 000002.2269936188.000000000306 0000.00000002.00000001.sdmp, S ampleRes.exe, 0000000A.0000000 2.2273974582.0000000002F20000. 00000002.00000001.sdmp, NlsDat a0414.exe, 0000000B.00000002.2 278988967.0000000003000000.000 00002.00000001.sdmp	false		high
http://https://pornthash.mobi/videos/tayna_tung%temp%/tmp_e473b4.exex	certutil.exe, 00000001.0000000 2.2223923762.0000000002770000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
177.130.51.198	unknown	Brazil		52747	WspServicosdeTelecomunicacoesLtdaBR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339446
Start date:	14.01.2021
Start time:	03:59:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample1.bin (renamed file extension from bin to doc)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@20/19@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 59.1% (good quality ratio 54.9%) • Quality average: 65.3% • Quality standard deviation: 27.9%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, rundll32.exe, conhost.exe • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:01:45	API Interceptor	223x Sleep call for process: svchost.exe modified
04:01:59	API Interceptor	11x Sleep call for process: tmp_e473b4.exe modified
04:02:01	API Interceptor	9x Sleep call for process: auditpolmsg.exe modified

Time	Type	Description
04:02:03	API Interceptor	10x Sleep call for process: wcnwiz.exe modified
04:02:05	API Interceptor	11x Sleep call for process: SampleRes.exe modified
04:02:08	API Interceptor	10x Sleep call for process: NlsData0414.exe modified
04:02:10	API Interceptor	11x Sleep call for process: mfc140.exe modified
04:02:12	API Interceptor	13x Sleep call for process: ieframe.exe modified
04:02:15	API Interceptor	11x Sleep call for process: cryptdll.exe modified
04:02:17	API Interceptor	204x Sleep call for process: wlanui.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
177.130.51.198	task5.doc	Get hash	malicious	Browse	
	P7Ya8tCZGu.exe	Get hash	malicious	Browse	
	A4Y5PZQuwQ.exe	Get hash	malicious	Browse	
	E8ykSGwVtp.exe	Get hash	malicious	Browse	
	Pc3hLrhR6C.exe	Get hash	malicious	Browse	
	MzQN95jvoX.exe	Get hash	malicious	Browse	
	77CJzpSlkv.exe	Get hash	malicious	Browse	
	AGWH4hi4Ig.exe	Get hash	malicious	Browse	
	1FFfIHDjlS.exe	Get hash	malicious	Browse	
	http://gestione.co/wp-content/lm/27649110/qnbbw9ja1scf-0040/	Get hash	malicious	Browse	
	http://gestione.co/wp-content/lm/27649110/qnbbw9ja1scf-0040/	Get hash	malicious	Browse	
	http://https://fiera-deutzfahr.com/wp-admin/Overview/6555921/6uw9g10b-0079388/	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WspServicosdeTelecomunicacoesLtdaBR	sample1.doc	Get hash	malicious	Browse	• 177.130.51.198
	task5.doc	Get hash	malicious	Browse	• 177.130.51.198
	P7Ya8tCZGu.exe	Get hash	malicious	Browse	• 177.130.51.198
	A4Y5PZQuwQ.exe	Get hash	malicious	Browse	• 177.130.51.198
	E8ykSGwVtp.exe	Get hash	malicious	Browse	• 177.130.51.198
	Pc3hLrhR6C.exe	Get hash	malicious	Browse	• 177.130.51.198
	MzQN95jvoX.exe	Get hash	malicious	Browse	• 177.130.51.198
	77CJzpSlkv.exe	Get hash	malicious	Browse	• 177.130.51.198
	AGWH4hi4Ig.exe	Get hash	malicious	Browse	• 177.130.51.198
	1FFfIHDjlS.exe	Get hash	malicious	Browse	• 177.130.51.198
	http://gestione.co/wp-content/lm/27649110/qnbbw9ja1scf-0040/	Get hash	malicious	Browse	• 177.130.51.198
	http://gestione.co/wp-content/lm/27649110/qnbbw9ja1scf-0040/	Get hash	malicious	Browse	• 177.130.51.198
	http://https://fiera-deutzfahr.com/wp-admin/Overview/6555921/6uw9g10b-0079388/	Get hash	malicious	Browse	• 177.130.51.198

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\Ksh1.pdf	sample1.doc	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sample1.doc	Get hash	malicious	Browse	
	task5.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0001.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	598272
Entropy (8bit):	5.856822353998229
Encrypted:	false
SSDEEP:	12288:FmkwUHZaSyYGKFaaGXuG7ttehnyragYqyPhU:FmkVZm2hnyDxAC
MD5:	7E9AB23E4F7C98AF0A03B64E3C14D7F6
SHA1:	BAD0DC91FB2929FDBF66E569257BABA97E1EC233
SHA-256:	532A6B3137804F51266923EBB06FA6DE43022C2B14F14F6785DDFDA8CA4238EE
SHA-512:	014420FD9C97DBCFF01E11E385E392D8F9AB91D238A418E76C72CD1CD191D2BEE17E7442398C20BA229AD25B0461778F76A88039B1810E20E88A0FE58C43478
Malicious:	false
Reputation:	low
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0002.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1191944
Entropy (8bit):	3.9253267830463896
Encrypted:	false
SSDEEP:	12288:ade8HF9kUxyxlFnsn4yA9W8MZ5axhVYGByJGZGy9e3rfTqtTfLlR1xwSaf67HNu4:me8HFmU/4yA9W89VYU7sY7yz1DsVirpI
MD5:	DA122309698B26E96848A6A829EEF5C1
SHA1:	DFA1B8C96C19827A595EEB15B2EC5386F9746CEF
SHA-256:	26585F7107FBECBA9F5282D4C1F1783441C60187057133121BD40D5C31C6149A
SHA-512:	4318F2A585966FC03A86D566819F06F15A93BE1616231FC34E4C5B7F0B6317083654B7F9C446D250D91C25176853B8CEB42504419D35ECD7F8DEC4C6048B5D7D
Malicious:	false
Preview:	T.V.q.Q.A.A.M.A.A.A.A.E.A.A.A.A./././.8.A.A.L.g.A.A.A.A.A.A.A.A.A.A.Q.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A. C.A.E.A.A.A.4.f.u.g.4.A.t.A.n.N.I.b.g.B.T.M.0.h.V.G.h.p.c.y.B.w.c.m.9.n.c.m.F.t.I.G.N.h.b.m.5.v.d.C.B.i.Z.S.B.y.d.W.4.g.a.W.4.g.R.E.9.T.I.G.1.v.Z.G.U.u.D.Q.0.K.J.A.A.A.A. A.A.A.A.A.A.p.T.i.i.j.b.S.9.G.8.G.0.v.R.v.B.t.L.0.b.w.2.b.O.3.8.G.c.v.R.v.D.Z.s.7.X.w.G.i.9.G.8.N.m.z.t.P.B.1.L.0.b.w.P.0.d.D.8.U.0.v.R.v.A./.R.0.L.x.Y.i.9.G.8.D.9.H.R.f. F.+.L.0.b.w.Z.F.f.V.8.G.g.v.R.v.B.t.L.0.f.w.C.S.9.G.8.P.d.G.T./.F.s.L.0.b.w.9.0.Z.G.8.W.w.v.R.v.D.3.R.r.n.w.b.C.9.G.8.G.0.v.0.f.B.s.L.0.b.w.9.0.Z.E.8.W.w.v.R.v.B.S.a.W.N. o.b.S.9.G.8.A.A.A.A.A.A.A.A.A.A.A.A.U.E.U.A.A.E.w.B.B.Q.A.r.7.Z.h.f.A.A.A.A.A.A.A.A.A.A.A.D.g.A.A.I.h.C.w.E.O.E.A.A.U.A.Q.A.A.x.A.U.A.A.A.A.A.A.G.R.9.A.A.A.A.E.A.A. A.A.D.A.B.A.A.A.A.A.B.A.A.E.A.A.A.A.A.I.A.A.A.U.A.A.Q.A.A.A.A.A.A.B.Q.A.B.A.A.A.A.A.A.A.A.E.A.c.A.A.A.Q.A.A.A.A.A.A.A.A.A.D.A.E.A.B.A.A.A.Q.A.A.A.Q.A.A.A.A.A.B.A. A.A.B.A.A.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0003.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	600580
Entropy (8bit):	5.850565167047853
Encrypted:	false
SSDEEP:	12288:nmkTbcqi+vjtKTA4rWgRRtgqDnygr6Yq/PWY:nmkvdbKDnyzx35
MD5:	1D35754EDB0B7AA76891735215FC048A
SHA1:	E0B1C34B3C39C1F097B7A3749174D098DC51E265
SHA-256:	C31DBCD8F7F979CB09159FE60B70A0C8F7A58C5E67EA8522E031F0BC5DF8A348
SHA-512:	6851E23E0FBFF103D5BDCE5CDC4D425C070D8E72BA66525CD2F85255F5BF3921C434C371B1459F184468546670AC26FD307035572E12DF84D1172517E8202A07
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0003.doc

Preview:

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy
Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U
0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAA
AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA
EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAABw
CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC
5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl
bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0005.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	598272
Entropy (8bit):	5.856822353998229
Encrypted:	false
SSDEEP:	12288:FmkwUHZaSyYGKFaaGXuG7ttehnyragYqyPhU:FmkVZm2hnyDxAC
MD5:	7E9AB23E4F7C98AF0A03B64E3C14D7F6
SHA1:	BAD0DC91FB2929FDBF66E569257BABA97E1EC233
SHA-256:	532A6B3137804F51266923EBB06FA6DE43022C2B14F14F6785DDFDA8CA4238EE
SHA-512:	014420FD9C97DBCFF01E11E385E392D8F9AB91D238A418E76C72CD1CD191D2BEE17E7442398C20BA229AD25B0461778F76A88039B1810E20E88A0FE58C43478
Malicious:	false

Preview:

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy
Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U
0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAA
AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA
EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAABw
CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC
5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl
bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0666.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1191944
Entropy (8bit):	3.9253267830463896
Encrypted:	false
SSDEEP:	12288:ade8HF9kUxyxlFnsn4yA9W8MZ5axhVYGByJGZGy9e3rfTqtTfLlR1xwSaf67HNu4:me8HFmU/4yA9W89VYU7sY7yz1DsVirpI
MD5:	DA122309698B26E96848A6A829EEF5C1
SHA1:	DFA1B8C96C19827A595EEB15B2EC5386F9746CEF
SHA-256:	26585F7107FBECBA9F5282D4C1F1783441C60187057133121BD40D5C31C6149A
SHA-512:	4318F2A585966FC03A86D566819F06F15A93BE1616231FC34E4C5B7F0B6317083654B7F9C446D250D91C25176853B8CEB42504419D35ECD7F8DEC4C6048B5D7D
Malicious:	false

Preview:

T.V.q.Q.A.A.M.A.A.A.A.E.A.A.A.A./././.8.A.A.L.g.A.A.A.A.A.A.A.A.A.A.Q.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.
C.A.E.A.A.A.4.f.u.g.4.A.t.A.n.N.I.b.g.B.T.M.0.h.V.G.h.p.c.y.B.w.c.m.9.n.c.m.F.t.I.G.N.h.b.m.5.v.d.C.B.i.Z.S.B.y.d.W.4.g.a.W.4.g.R.E.9.T.I.G.1.v.Z.G.U.u.D.Q.0.K.J.A.A.A.A.A.
A.A.A.A.A.A.p.T.i.i.j.b.S.9.G.8.G.0.v.R.v.B.t.L.0.b.w.2.b.O.3.8.G.c.v.R.v.D.Z.s.7.X.w.G.i.9.G.8.N.m.z.t.P.B.1.L.0.b.w.P.0.d.D.8.U.0.v.R.v.A./.R.0.L.x.Y.i.9.G.8.D.9.H.R.f.
F.+.L.0.b.w.Z.F.f.V.8.G.g.v.R.v.B.t.L.0.f.w.C.S.9.G.8.P.d.G.T./.F.s.L.0.b.w.9.0.Z.G.8.W.w.v.R.v.D.3.R.r.n.w.b.C.9.G.8.G.0.v.0.f.B.s.L.0.b.w.9.0.Z.E.8.W.w.v.R.v.B.S.a.W.N.
o.b.S.9.G.8.A.A.A.A.A.A.A.A.A.A.A.A.A.A.U.E.U.A.A.E.w.B.B.Q.A.r.7.Z.h.f.A.A.A.A.A.A.A.A.A.A.A.A.D.g.A.A.I.h.C.w.E.O.E.A.A.U.A.Q.A.A.x.A.U.A.A.A.A.A.A.A.G.R.9.A.A.A.A.E.A.A.
A.A.D.A.B.A.A.A.A.A.A.B.A.A.E.A.A.A.A.A.A.I.A.A.A.U.A.A.Q.A.A.A.A.A.A.A.B.Q.A.B.A.A.A.A.A.A.A.A.A.A.E.A.c.A.A.A.Q.A.A.A.A.A.A.A.A.A.A.D.A.E.A.B.A.A.A.Q.A.A.A.Q.A.A.A.A.A.A.B.A.
A.A.B.A.A.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0798.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	600580
Entropy (8bit):	5.850565167047853
Encrypted:	false
SSDEEP:	12288:nmkTbcqi+vjtKTA4rWgRRtgqDnygr6Yq/PWY:nmkvdbKDnyzx35
MD5:	1D35754EDB0B7AA76891735215FC048A
SHA1:	E0B1C34B3C39C1F097B7A3749174D098DC51E265
SHA-256:	C31DBCD8F7F979CB09159FE60B70A0C8F7A58C5E67EA8522E031F0BC5DF8A348
SHA-512:	6851E23E0FBFF103D5BDCE5CDC4D425C070D8E72BA66525CD2F85255F5BF3921C434C371B1459F184468546670AC26FD307035572E12DF84D1172517E8202A07
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0798.doc	
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{35EB0BAB-3BC6-4A41-A07F-15EEA53DBB38}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbC:IiiiiiiiifdLloZQc8++lsJe1MzNn
MD5:	EAA701BCC2359F9297273D117620CA80
SHA1:	D9E2AC26703E2668720A5B3E796DF52F3F52674A
SHA-256:	497E3B43D545A03EE2E00324DEAC332FD13FF811F41B42F881BCAD29AE14250D
SHA-512:	6F4F6936A2D454FABE565A177322B84A853DE887CBF1B10ECBFFF9D7755465AE60BFCBE66F4F949D986D103F12550B5160F614A74729DE0838DC451C76757491
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A... ...."...&...*.......:...>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B5C9B88B-61BE-41BF-89DB-AF92964D1C77}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Ksh1.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=Thu Jan 14 11:01:41 2021, mtime=Thu Jan 14 11:01:41 2021, atime=Thu Jan 14 11:01:42 2021, length=595972, window=hide
Category:	dropped
Size (bytes):	3660
Entropy (8bit):	4.4870215514715746
Encrypted:	false
SSDEEP:	96:87k/XicyByK27k/XicyByK2vk/X/c1O2vk/X/c12:87Iu27Iu2v51pv512
MD5:	5C048363FB804C47823972D53B75D3A5
SHA1:	FF2FD7DCCF53FA0A6F7E4DED1080C26A6A8F97AE
SHA-256:	FE5D58BEC071D21ECEAD746CFCF14EEC223B18E18282DECB92D49CB8607885AA
SHA-512:	D74E71166AB2CEA9A0093A59D043E3D65E219E8376D34D3D3721FEBFDB916A2B1AF68D9221AC11DB1824FAF78EBD32865403404B7049EB7ED23339BB6B1AB1F B
Malicious:	false
Preview:	L..................F.... ...;2B.m...;2B.m....M..m...........................q....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.....x.1......R6`..Public..b.......:...R6`*...b...............8.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....V.2......R6` .Ksh1.xls..>.......R5`.R5`*...;.....................K.s.h.1. ..x.l.s.......k...............-...8...[............?J......C:\Users\..#..................\\424505\Users.Public\Ksh1.xls.!.....\.....\.....\.....\.....\.....\.P.u.b.l.i.c.\.K.s.h.1...x.l.s..........................v..*.c M.jVD.Es................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.......424505....... ...D_....3N...W...9H.C...........[D_....3N...W...9H.C...........[....L..................F.... ...;2B.m...;2B.m....M..m...........................q....P.O.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Public.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, Read-Only, Directory, ctime=Tue Jul 14 02:20:08 2009, mtime=Thu Jan 14 11:01:41 2021, atime=Thu Jan 14 11:01:41 2021, length=4096, window=hide
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	4.462420567483035
Encrypted:	false
SSDEEP:	24:8L/XRlekwvB3qcL7Y2//XRlekwvB3qcL7c:8L/XjVFcfY2//XjVFcfc
MD5:	13715C1A57AC925C6D3529F23D8A0489
SHA1:	7475EF6A91727FD8449840C0B783B3FD34D5D7F1
SHA-256:	29832B00F50E3D4E063F7C97E2430C5A0F833CB5D3A2E66C1DFE2AE990C94832
SHA-512:	4137D28186FA2B19F766D33C5592236A59535C50A60FADBB48C5FAB332596C6FF17C45EFE460846E64F9755D5C911CD5B06F0CBA80EE9A185648D3B497EE854F
Malicious:	false
Preview:	L.....F.....1...;2B.m...;2B.m.....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.....x.1.....>.C..Public..b.....:...>.C*...b.....8.....P.u.b.l.i.c...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.6.....b.....-...8...[.....?J.....C:\Users\..#.....\\424505\Users.Public.....\....\....\....\....\....\.P.u.b.l.i.c.....v..*.cM.jVD.Es.....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.....424505.....D_....3N...W...9G.C.....[D_....3N...W...9G.C.....[....L.....F.....1....3..m....3..m.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@

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):	438
Entropy (8bit):	4.369509432724656
Encrypted:	false
SSDEEP:	6:M6dYrtg9CMdg9CMdg9UYrtg9CMUg9UYrhMUg9CMRMUg9s:M6IgEEgEEgJgEtg9tgEytgC
MD5:	9DDA3519F04FDEEB47B198EDD010E507
SHA1:	AC6C4075745C0F0064ADED9504934DDA44CB30E9
SHA-256:	A677F9380C0B0EB229D861D18FDDFFD4642FFCAF1ABF9007A77EC37F05F0BDBC
SHA-512:	8C0372F4659764915EC4D9EBA74F71E4464F1E5C56A0B31AF05638A747790B9AD2834642D94EB0512AEA1B5D8E292D9CB0029A849A0C91244376A50EC6501667
Malicious:	false
Preview:	[doc]..sample1.LNK=0..sample1.LNK=0..[doc]..sample1.LNK=0..Public.LNK=0..[doc]..sample1.LNK=0..[xls]..Ksh1.LNK=0..Ksh1.LNK=0..[doc]..sample1.LNK=0..[xls]..Ksh1.LNK=0..Ksh1.LNK=0..[doc]..sample1.LNK=0..[xls]..Ksh1.LNK=0..Public.LNK=0..[doc]..sample1.LNK=0..[xls]..Ksh1.LNK=0..Ksh1.LNK=0..[xls]..Ksh1.LNK=0..Public.LNK=0..[doc]..sample1.LNK=0..Ksh1.LNK=0..[xls]..Ksh1.LNK=0..Ksh1.LNK=0..[doc]..sample1.LNK=0..Ksh1.LNK=0..[xls]..Ksh1.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\sample1.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=Thu Jan 14 11:00:31 2021, mtime=Thu Jan 14 11:00:31 2021, atime=Thu Jan 14 11:00:33 2021, length=856064, window=hide
Category:	dropped
Size (bytes):	1994
Entropy (8bit):	4.504905520297006
Encrypted:	false
SSDEEP:	48:8C/XT3lTfhclhVMDlOcQh2C/XT3lTfhclhVMDlOcQ/:8C/XLIT5UcQh2C/XLIT5UcQ/
MD5:	2EAF88677CD16A68B2CD4263BA9E7CE0
SHA1:	AA9B6C640105E9474BABBF76571C364926445178
SHA-256:	919A3D28BFBE2D4CE57DCF0A8B1400DB858BAD490FEB436C3F4EFE343EB262BB
SHA-512:	7AA17F78876C1B55BBA4C8973D8420992E1C53D54667848D84B7857C6D066862C1AE9D2B83DE5A525DD45B0B6FFBF19B2D89372A42BC63A4E5BA0E2296D5140
Malicious:	false
Preview:	L.....F.... ....hv.l....hv.l.....l.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R.`..Desktop.d.....QK.X.R.`*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....^.2.....R.` .sample1.doc.D.....R.`.R.`*...?.....s.a.m.p.l.e.1...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\424505\Users.user\Desktop\sample1.doc."....\....\....\....\....\.D.e.s.k.t.o.p.\.s.a.m.p.l.e.1...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.....424505.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L..

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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Desktop\~$ample1.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\Ksh1.pdf	
Process:	C:\Windows\System32\certutil.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	446976
Entropy (8bit):	7.675102075961339
Encrypted:	false
SSDEEP:	12288:NWSikkQXsGOCAStP1W+TXPc9JXvaWv7j3:ESiL5Sp1W+TYfHj
MD5:	706EA7F029E6BC4DBF845DB3366F9A0E
SHA1:	942443DFB8784066523DB761886115E08C99575F
SHA-256:	FB07F875DC45E6045735513E75A83C50C78154851BD23A645D43EA853E6800AC
SHA-512:	036D5DE7E732302EF81989FBA62ABB1375119FC8141748D6548ED2310E95BDC07468ADA5CBF06C4F721B2B95CAF51E3267D4EF6DB2A2031CF5C8B2ABEE1C153
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 41%, Browse • Antivirus: ReversingLabs, Detection: 64%
Joe Sandbox View:	• Filename: sample1.doc, Detection: malicious, Browse • Filename: sample1.doc, Detection: malicious, Browse • Filename: task5.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)N(.m/F.m/F.m/F....g/F...../F....u/F.?GC.M/F.?GB.b/F.?GE.~/F.dW..h/F.m/G../F..FO.l/F..FF.l/F..F..l/F.m/..l/F..FD.l/F.Richm/F.....PE..L...+._.....!.....d}.....0.....@.....H...X...<.....PB.....0|..8.....h|..@.....0..8.....text...g..... ..`.rdata..d\...0...^.....@..@.data.....v.....@....rsrc...PB.....D...~.....@..@.reloc.....@..B.....

C:\Users\Public\~$Ksh1.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIlD9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\~$Ksh1.xls	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IlID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891 C
Malicious:	false
Preview:	.user...A.l.b.u.s.............p.........w...............w.............P.w..............w.....z.........w.....x...

C:\Users\Public\~WRD0000.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	595972
Entropy (8bit):	5.85065356609278
Encrypted:	false
SSDEEP:	12288:FmkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCY:FmkvVW9gnyQxt9
MD5:	D631AB4CEFF199B52FF4E4B7AAD0199D
SHA1:	F30002C31BF32184507182100942A2012F0B8703
SHA-256:	9DE083F693C144A38D697089F6560A2EFE81B1AD1C5385EC07D6B41BB54B8FFE
SHA-512:	56B3941CD93658F7DF8976213E2DFD5CB74E7ABB651AD26FDA9B7191E675E03289366B32EEDF68D139562A88DBBAE2589FDA8ABBDB756C43E2E605863459A16 2
Malicious:	false
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\Public\~WRD0004.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	595972
Entropy (8bit):	5.85065356609278
Encrypted:	false
SSDEEP:	12288:FmkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCY:FmkvVW9gnyQxt9
MD5:	D631AB4CEFF199B52FF4E4B7AAD0199D
SHA1:	F30002C31BF32184507182100942A2012F0B8703
SHA-256:	9DE083F693C144A38D697089F6560A2EFE81B1AD1C5385EC07D6B41BB54B8FFE
SHA-512:	56B3941CD93658F7DF8976213E2DFD5CB74E7ABB651AD26FDA9B7191E675E03289366B32EEDF68D139562A88DBBAE2589FDA8ABBDB756C43E2E605863459A16 2
Malicious:	false
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: User, Template: Normal.dotm, Last Saved By: kirin, Revision Number: 7, Name of Creating Application: Microsoft Office Word, Total Editing Time: 20:00, Create Time/Date: Sun May 10 01:31:00 2020, Last Saved Time/Date: Wed Oct 28 04:44:00 2020, Number of Pages: 2, Number of Words: 89482, Number of Characters: 510049, Security: 0
Entropy (8bit):	6.919205506848504
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	sample1.doc
File size:	850432
MD5:	7dbd8ecfada1d39a81a58c9468b91039
SHA1:	0d21e2742204d1f98f6fcabe0544570fd6857dd3
SHA256:	dc40e48d2eb0e57cd16b1792bdccc185440f632783c7bcc87c955e1d4e88fc95
SHA512:	a851ac80b43ebdb8e990c2eb3daabb456516fc40bb43c9f76d0112674dbd6264efce881520744f0502f2962fc0bb4024e7d73ea66d56bc87c0cc6dfde2ab869a
SSDEEP:	12288:emkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCspBZZLFLIx/mBDOq1a:emkvVW9gnyQxtN9eEBDOQa
File Content Preview:	.....>.....g.....j.....Z...[...\...]...^..._...`...a...b...c...d...e...f.....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "sample1.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	
Subject:	
Author:	User
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	kirin
Revion Number:	7
Total Edit Time:	1200
Create Time:	2020-05-10 00:31:00

Summary	
Last Saved Time:	2020-10-28 04:44:00
Number of Pages:	2
Number of Words:	89482
Number of Characters:	510049
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	4250
Number of Paragraphs:	1196
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 3696

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	3696
Data ASCII:	. . . . . { . . . . . ' E . . . . . (. . . . . 2 . . . . . S l e e p . . . . . x . . . . . M E . .
Data Raw:	01 16 03 00 00 18 01 00 00 dc 06 00 00 fc 00 00 00 02 02 00 00 ff ff ff ff e3 06 00 00 7b 0b 00 00 00 00 00 00 01 00 00 00 f1 27 45 f5 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 28 00 00 00 00 00 32 02 20 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 6c 65 65 70 00 00 00 00 ff ff ff ff 01 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
#Else
VB_Name
VB_Creatable
".pdf"):
SetTask(Task
VB_Exposed
Null,
Form_Close()
("doc"):
Formt,
VB_TemplateDerived
Function
(ByVal
String
Right(Range.Text,
String)
Form_Close
Long)
Long,
VB_Customizable
Task,
("xls"):
FileName:=STP
".xls
PtrSafe
Left(ActiveDocument.Paragraphs(One).Range.Text,
Declare
"ThisDocument"
SetTask

Keyword
False
FileFormat:=wdFormatText
Attribute
Private
VB_PredeclaredId
Sleep
VB_GlobalNameSpace
VB_Base
".pdf,ln")
Document_Close()

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651
Base64 Encoded:	True
Data ASCII:	. . . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.25569624217
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . . ? ! . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.473780805052
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . l . . . . . (. . . . . 4 . . . . . @ . . . . . L . . . . . T . . . . . \\ . . . . . d . . . . . U s e r . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 6c 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 c0 00 00 00 06 00 00 00 cc 00 00 00 07 00 00 00 d8 00 00 00 08 00 00 00 ec 00 00 00 09 00 00 00 fc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7386

General	
Stream Path:	1Table

General	
File Type:	data
Stream Size:	7386
Entropy:	5.92077573609
Base64 Encoded:	True
Data ASCII:	. . . . . x . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	1e 06 0f 00 12 00 01 00 78 01 0f 00 07 00 03 00 03 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 187989

General	
Stream Path:	Data
File Type:	data
Stream Size:	187989
Entropy:	7.97862280177
Base64 Encoded:	True
Data ASCII:	U . . . D . d . . . . . 1 . . . . . N . . . . . C . . . * . . . . A . . . . . t . e . m . p . l . a . t . e . . . . . b . . . . . b r . . . . 7 . a . _ . . . . . D . . . . . n . . . . . b r . . . . 7 . a . _ . . . . P N G . . . . . I H D R . . . O . . . . . 3 0 . u
Data Raw:	55 de 02 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 a3 31 e3 1d c3 03 c3 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 4e 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 43 00 0b f0 2a 00 00 00 04 41 01 00 00 00 05 c1 12 00 00 00 06 01 02 00 00 00 ff 01 00 00 08 00 74 00 65 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 367

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	367
Entropy:	5.29037636248
Base64 Encoded:	True
Data ASCII:	I D = " { D 4 7 2 8 3 5 A - 3 8 9 1 - 4 D B 9 - 8 6 F 0 - 0 C 1 2 4 A F F D 6 E 1 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 8 0 A E 9 E F E D E F E D E F E D E F E D " . . D P B = " 9 6 9 4 7 7 F B 8 B 0 7 1 8 0 8 1 8 0 8 1 8 " . . G C = " 2 4 2 6 C 5 8 9 D D 1 6 D E 1 6 D E E 9 " . . . . [H o s t E x t e n d e r I n f o]
Data Raw:	49 44 3d 22 7b 44 34 37 32 38 33 35 41 2d 33 38 39 31 2d 34 44 42 39 2d 38 36 46 30 2d 30 43 31 32 34 41 46 46 44 36 45 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2845

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2845
Entropy:	4.32828178006
Base64 Encoded:	False

General	
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 513

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	513
Entropy:	6.25624133358
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . Y { . ` . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ S y s t e m 3 . 2 \\ . e 2 . t l b . # O L E  A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . * . \\ C . . . . . . m . . .
Data Raw:	01 fd b1 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 59 7b a3 60 0a 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: WordDocument, File Type: data, Stream Size: 627764

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	627764
Entropy:	6.04018774642
Base64 Encoded:	False
Data ASCII:	. . . . { . . . . - . . . . b j b j . . . . 4 . . . . . . f . . . % . . . . F . . . . F . . . .
Data Raw:	ec a5 c1 00 7b 00 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 eb 2d 09 00 0e 00 62 6a 62 6a 84 bd 84 bd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 34 94 09 00 e6 d7 d5 66 e6 d7 d5 66 eb 25 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/21-04:02:18.387074	TCP	2404310	ET CNC Feodo Tracker Reported CnC Server TCP group 6	49170	80	192.168.2.22	177.130.51.198
01/14/21-04:02:20.339180	ICMP	449	ICMP Time-To-Live Exceeded in Transit			177.130.48.10	192.168.2.22
01/14/21-04:02:23.401000	ICMP	449	ICMP Time-To-Live Exceeded in Transit			177.130.48.10	192.168.2.22

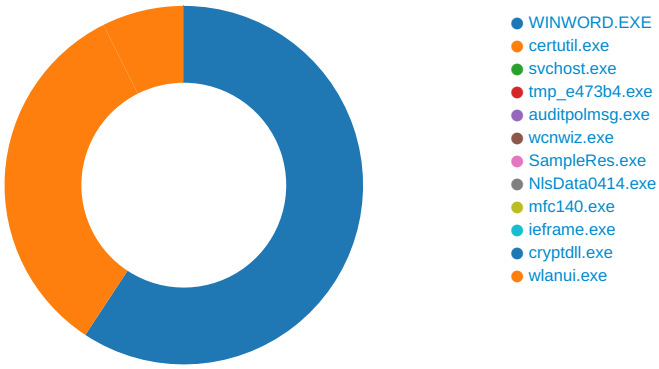
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 04:02:18.387073994 CET	49170	80	192.168.2.22	177.130.51.198
Jan 14, 2021 04:02:21.448874950 CET	49170	80	192.168.2.22	177.130.51.198

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2264 Parent PID: 584

General

Start time:	04:00:33
Start date:	14/01/2021
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:	0x13fe60000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF9A38BB9DE8B04B68.TMP	success or wait	1	7FEE90A9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	7FEE903EC53	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE9046CAC	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F364C	success or wait	1	7FEE90A9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F364C	F364C	binary	04 00 00 00 D8 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 45 55 EF 6C EA D6 01 4C 36 0F 00 4C 36 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378746414	1378746415	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1378746415	1378746416	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F364C	F364C	binary	04 00 00 00 D8 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 74 45 55 EF 6C EA D6 01 4C 36 0F 00 4C 36 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 D8 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4C 36 0F 00 4C 36 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: certutil.exe PID: 2440 Parent PID: 1220

General

Start time:	04:01:43
Start date:	14/01/2021
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf
Imagebase:	0xff9a0000
File size:	1192448 bytes
MD5 hash:	4586B77B18FA9A8518AF76CA8FD247D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\cerED0D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FFA51B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cerED0D.tmp	success or wait	1	FFA51B34	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2348 Parent PID: 428

General

Start time:	04:01:45
Start date:	14/01/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff0e0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: tmp_e473b4.exe PID: 1772 Parent PID: 3052

General

Start time:	04:01:57
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\tmp_e473b4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp/tmp_e473b4.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2256698017.00000000003F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000003.2252976219.0000000000588000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.2256830860.0000000000586000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: auditpolmsg.exe PID: 1688 Parent PID: 1772

General

Start time:	04:01:59
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\srclient\auditpolmsg.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\srclient\auditpolmsg.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000003.2257551859.00000000005F8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2263042599.00000000005F6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2262078055.0000000000361000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wcnwiz.exe PID: 2064 Parent PID: 1688

General

Start time:	04:02:01
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\mfc110\wcnwiz.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mfc110\wcnwiz.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000003.2262096055.0000000000548000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2265953499.0000000000546000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2265821061.00000000003B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SampleRes.exe PID: 2004 Parent PID: 2064

General

Start time:	04:02:04
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\capiprovider\SampleRes.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\capiprovider\SampleRes.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000003.2266631097.0000000000578000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2271093826.0000000000576000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2271279815.00000000007B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NlsData0414.exe PID: 2364 Parent PID: 2004

General

Start time:	04:02:06
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\RMActivate_ssp_isv\NlsData0414.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\RMActivate_ssp_isv\NlsData0414.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2275531038.00000000002B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2276502729.00000000005E6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000003.2271289978.00000000005E8000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mfc140.exe PID: 1664 Parent PID: 2364

General

Start time:	04:02:08
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\KBDNO\mfc140.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\KBDNO\mfc140.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2279698396.00000000003E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000003.2276010487.00000000005F8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2280282398.00000000005F6000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieframe.exe PID: 1236 Parent PID: 1664

General

Start time:	04:02:10
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\advapi32\ieframe.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\advapi32\ieframe.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2285331820.00000000008E4000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000003.2280766001.0000000000928000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2285132994.0000000000321000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cryptdll.exe PID: 2728 Parent PID: 1236

General

Start time:	04:02:13
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\nshipsec\cryptdll.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\nshipsec\cryptdll.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2292365132.00000000008C4000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000003.2286180989.0000000000908000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2292162710.0000000000621000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanui.exe PID: 2832 Parent PID: 2728

General

Start time:	04:02:15
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\DShowRdpFilter\wlanui.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\DShowRdpFilter\wlanui.exe
Imagebase:	0x400000
File size:	344110 bytes
MD5 hash:	E87553AEBAC0BF74D165A87321C629BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2335114479.00000000002B4000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2335374791.0000000000481000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000003.2292126114.00000000002F8000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	482FB8	HttpSendRequestW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis