ID: 425356
Sample Name: sample1.bin
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 00:16:20
Date: 27/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

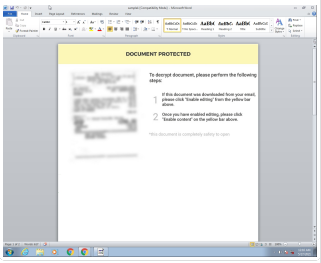
Analysis Report sample1.bin

Overview

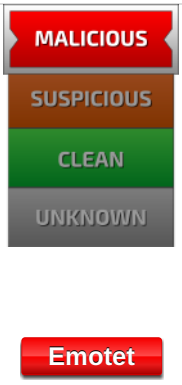
General Information

Sample Name:	sample1.bin (renamed file extension from bin to doc)
Analysis ID:	425356
MD5:	7dbd8ecfada1d39.
SHA1:	0d21e2742204d1..
SHA256:	dc40e48d2eb0e5..
Infos:	

Most interesting Screenshot:



Detection



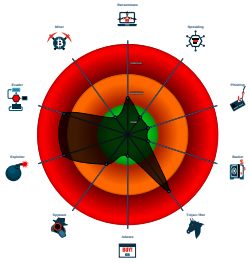
Emotet

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Creates and opens a fake document…
- Creates processes via WMI
- Document contains an embedded VB…
- Drops PE files to the user root direc…
- Drops executables to the windows d…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1492 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- certutil.exe (PID: 2336 cmdline: Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf MD5: 4586B77B18FA9A8518AF76CA8FD247D9)
- svchost.exe (PID: 2904 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- tmp_e473b4.exe (PID: 1872 cmdline: C:\Users\user\AppData\Local\Temp/tmp_e473b4.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
  - normaliz.exe (PID: 2400 cmdline: C:\Windows\SysWOW64\mfcm140\normaliz.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
    - mmcshext.exe (PID: 2496 cmdline: C:\Windows\SysWOW64\clip\mmcshext.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
      - ir50_qcx.exe (PID: 2104 cmdline: C:\Windows\SysWOW64\regedt32\ir50_qcx.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
        - dhcpcmonitor.exe (PID: 2552 cmdline: C:\Windows\SysWOW64\KBDNEPR\dhcpcmonitor.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
          - adsmsext.exe (PID: 1616 cmdline: C:\Windows\SysWOW64\api-ms-win-core-interlocked-l1-1-0\adsmsext.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
            - TSChannel.exe (PID: 2856 cmdline: C:\Windows\SysWOW64\oleaccrc\TSChannel.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
              - qdvd.exe (PID: 2748 cmdline: C:\Windows\SysWOW64\iprtrmgr\qdvd.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
                - msvcp120_clr0400.exe (PID: 1036 cmdline: C:\Windows\SysWOW64\whhelper\msvcp120_clr0400.exe MD5: E87553AEBAC0BF74D165A87321C629BE)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAM/TXLLvX91I6dVMYe+T1PPO6mpcg7OJ\ncMl9o/g4nUhZOp8fAAmQl8XMXeGvDhZXTyX1AXf401iPFui0RB6glhl/7/djvi7j\nl32lAhyBANpKGty8xf3J5kGwwClnG/CXHQIDAQAB",
  "C2 list": [
    "177.130.51.198:80",
    "91.121.87.90:8080",
    "104.131.144.215:8080",
    "188.226.165.170:8080",
    "2.58.16.86:8080",
    "79.133.6.236:8080",
    "125.200.20.233:80",
    "109.206.139.119:80",
    "188.40.170.197:80",
    "121.117.147.153:443",
    "221.147.142.214:80",
    "88.247.58.26:80",
```

```
    "37.205.9.252:7080",
    "213.165.178.214:80",
    "27.83.209.210:443",
    "24.231.51.190:80",
    "192.210.217.94:8080",
    "123.216.134.52:80",
    "179.5.118.12:80",
    "103.80.51.61:8080",
    "172.96.190.154:8080",
    "223.17.215.76:80",
    "46.105.131.68:8080",
    "116.91.240.96:80",
    "118.243.83.70:80",
    "190.117.101.56:80",
    "103.229.73.17:8080",
    "5.79.70.250:8080",
    "172.105.78.244:8080",
    "95.76.142.243:80",
    "113.193.239.51:443",
    "113.161.148.81:80",
    "180.148.4.130:8080",
    "172.193.79.237:80",
    "42.200.96.63:80",
    "110.37.224.243:80",
    "212.198.71.39:80",
    "185.80.172.199:80",
    "153.229.219.1:443",
    "162.144.145.58:8080",
    "190.55.186.229:80",
    "94.212.52.40:80",
    "37.46.129.215:8080",
    "82.78.179.117:443",
    "58.27.215.3:8080",
    "178.33.167.120:8080",
    "190.164.135.81:80",
    "73.100.19.104:80",
    "157.7.164.178:8081",
    "115.79.59.157:80",
    "190.194.12.132:80",
    "85.75.49.113:80",
    "185.142.236.163:443",
    "113.203.238.130:80",
    "91.75.75.46:80",
    "41.185.29.128:8080",
    "185.208.226.142:8080",
    "188.166.220.180:7080",
    "109.13.179.195:80",
    "91.83.93.103:443",
    "190.151.5.131:443",
    "203.153.216.178:7080",
    "51.38.50.144:8080",
    "36.91.44.183:80",
    "78.186.65.230:80",
    "180.23.53.200:80",
    "73.55.128.120:80",
    "75.127.14.170:8080",
    "119.92.77.17:80",
    "192.241.220.183:8080",
    "120.51.34.254:80",
    "202.29.237.113:8080",
    "41.76.213.144:8080",
    "195.201.56.70:8080",
    "175.103.38.146:80",
    "190.192.39.136:80",
    "203.56.191.129:8080",
    "180.21.3.52:80",
    "50.116.78.109:8080",
    "47.154.85.229:80",
    "54.38.143.245:8080",
    "43.255.175.197:80",
    "60.125.114.64:443",
    "8.4.9.137:8080",
    "91.213.106.100:8080",
    "116.202.10.123:8080",
    "103.93.220.182:80",
    "115.79.195.246:80",
    "139.59.61.215:443",
    "45.239.204.100:80",
    "143.95.101.72:8080",
    "198.20.228.9:8080",
    "192.163.221.191:8080",
    "139.59.12.63:8080",
    "77.74.78.80:443",
    "118.33.121.37:80",
    "126.126.139.26:443",
    "46.32.229.152:8080",
    "74.208.173.91:8080",
    "190.85.46.52:7080",
    "37.187.100.220:7080"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.2260910791.0000000000688000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000D.00000003.2274679265.00000000005B8000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000B.00000002.2269436388.0000000000331000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000F.00000002.2289663022.00000000005B6000.00000004.00000020.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000000C.00000002.2274011391.00000000004F1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

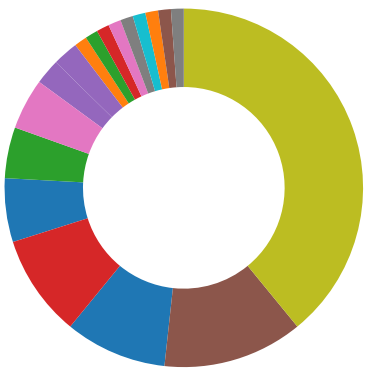
Unpacked PEs

Source	Rule	Description	Author	Strings
13.3.adsmsext.exe.5b8ab8.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
10.2.mmcshext.exe.688500.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
13.2.adsmsext.exe.5b8ab8.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
16.3.msvcp120_clr0400.exe.2f8598.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
8.2.tmp_e473b4.exe.9285b8.3.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 40 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

Found malware configuration

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:

C2 URLs / IPs found in malware configuration

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)

Stealing of Sensitive Information:

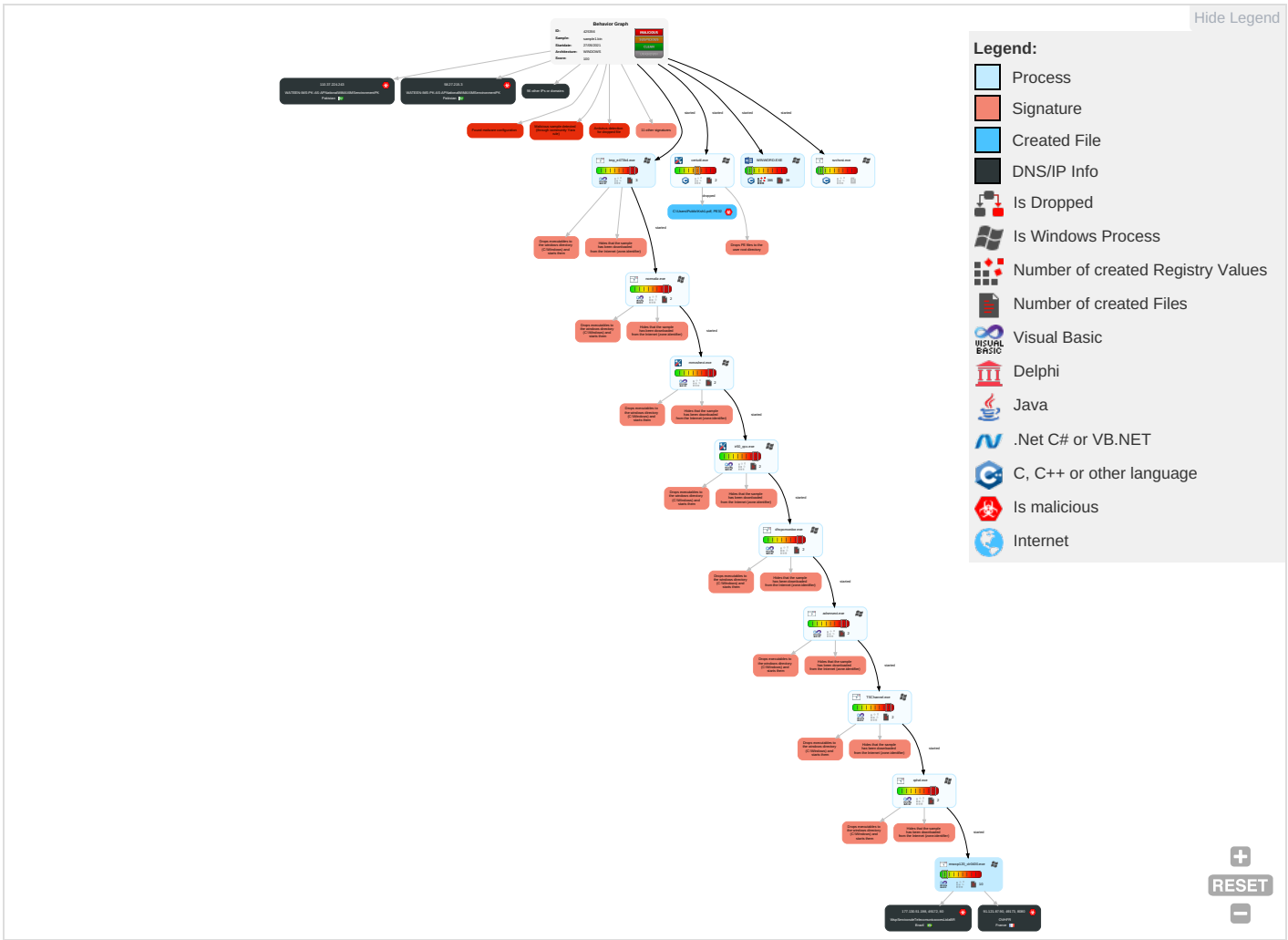
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
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 3	
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	
Domain Accounts	Exploitation for Client Execution 1 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	Non-Standard Port 1	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	I
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 1 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	
Cloud Accounts	Service Execution 1 1	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 2	
Replication Through Removable Media	Launchd	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	
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	
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	
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	

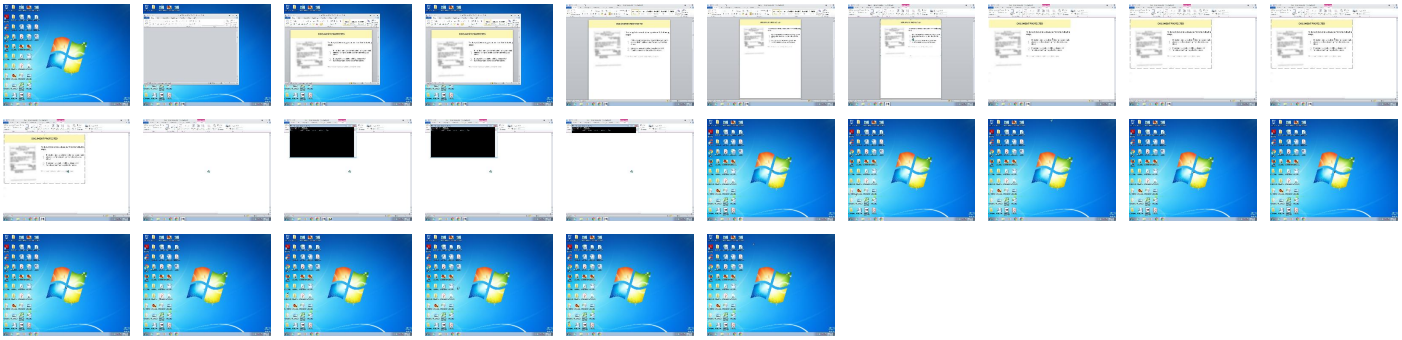
Behavior Graph

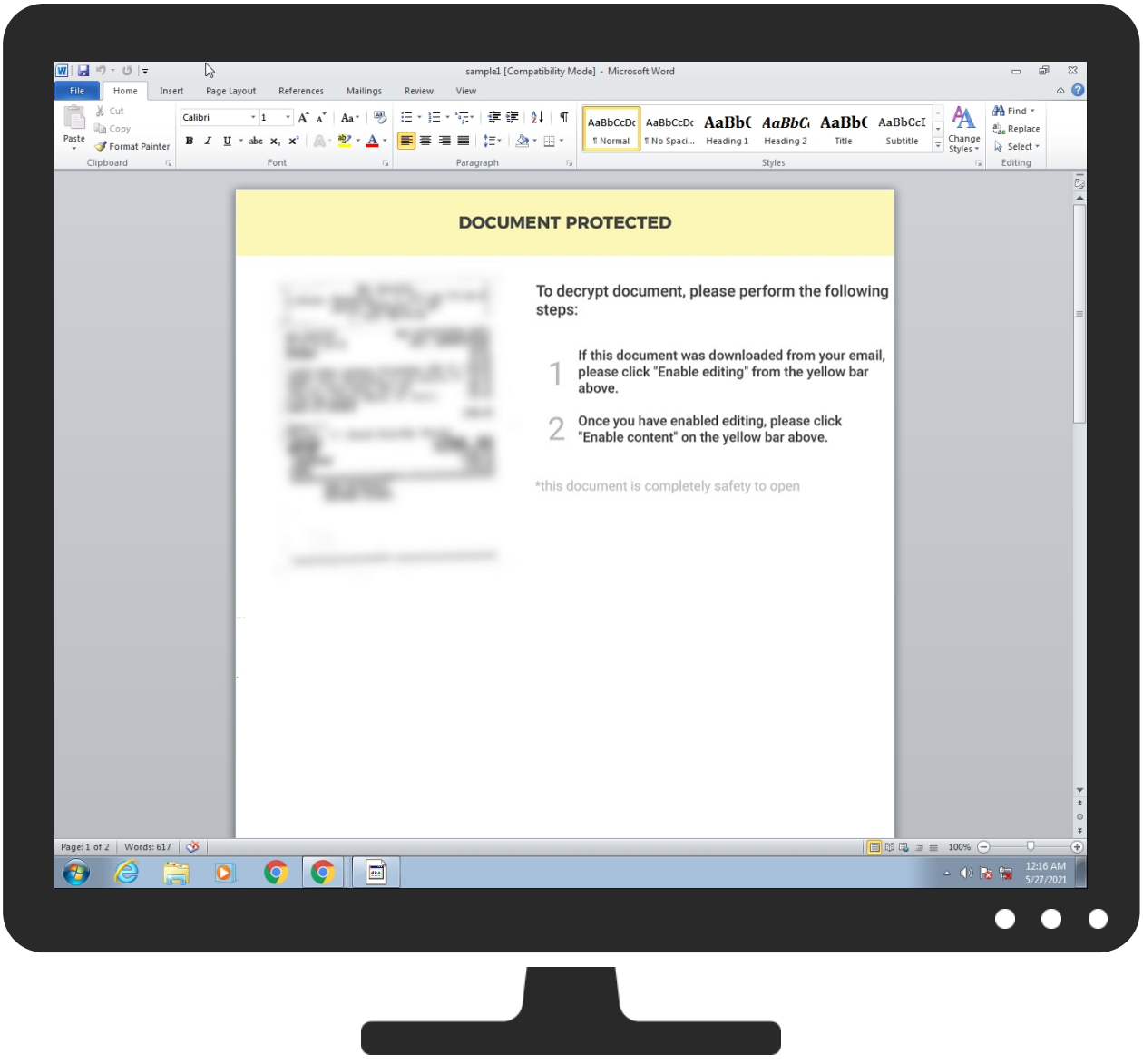


Screenshots

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	57%	Virustotal		Browse
sample1.doc	46%	Metadefender		Browse
sample1.doc	68%	ReversingLabs	Document-Word.Trojan.Valyria	

Source	Detection	Scanner	Label	Link
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		
C:\Users\Public\Ksh1.pdf	41%	Metadefender		Browse
C:\Users\Public\Ksh1.pdf	67%	ReversingLabs	Win32.Trojan.Casdet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.1.TSChannel.exe.39a0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.dhcpcmonitor.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
14.0.TSChannel.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
14.2.TSChannel.exe.2b8550.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.3.adsmsext.exe.5b8ab8.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.0.mmcshext.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
8.0.tmp_e473b4.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
8.3.tmp_e473b4.exe.9285b8.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.adsmsext.exe.290000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.mmcshext.exe.688500.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.ir50_qcx.exe.330000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.1.mmcshext.exe.3980000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.3.normaliz.exe.658540.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.1.dhcpcmonitor.exe.39e0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.msvcp120_clr0400.exe.2f8598.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.ir50_qcx.exe.548548.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.adsmsext.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
11.1.ir50_qcx.exe.3980000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.tmp_e473b4.exe.640000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.1.normaliz.exe.3a10000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.normaliz.exe.3f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.3.TSChannel.exe.2b8550.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.adsmsext.exe.5b8ab8.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.tmp_e473b4.exe.9285b8.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.0.qdvd.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
12.3.dhcpcmonitor.exe.2f8560.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.qdvd.exe.3f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.qdvd.exe.5b8518.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.TSChannel.exe.1c60000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.0.normaliz.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
15.3.qdvd.exe.5b8518.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.ir50_qcx.exe.548548.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.dhcpcmonitor.exe.2f8560.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.mmcshext.exe.688500.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.ir50_qcx.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
10.2.mmcshext.exe.3f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.1.tmp_e473b4.exe.39b0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.1.adsmsext.exe.2ca0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.normaliz.exe.658540.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.dhcpcmonitor.exe.4f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.1.TSChannel.exe.39a0000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.msvcp120_clr0400.exe.470000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.msvcp120_clr0400.exe.400000.0.unpack	100%	Avira	TR/AD.Emotet.fao		Download File
16.3.msvcp120_clr0400.exe.2f8598.0.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%	Virustotal		Browse
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	
http://91.121.87.90:8080/KFDwQljVkxD3/OOFcmzcP5LKdqC/7kx60YXntHFlDt/5Rmtlx5Mir4E2nTGMFj/vs6RDbQfHrygTYrl/	0%	Avira URL Cloud	safe	
http://177.130.51.198/43z7rPqPirmV4qB/AthcoPDmU/Q4ILc7kQKSHycUR/pIpU/8iSRPWx/wgrz9ygVvehFY9FxG0/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

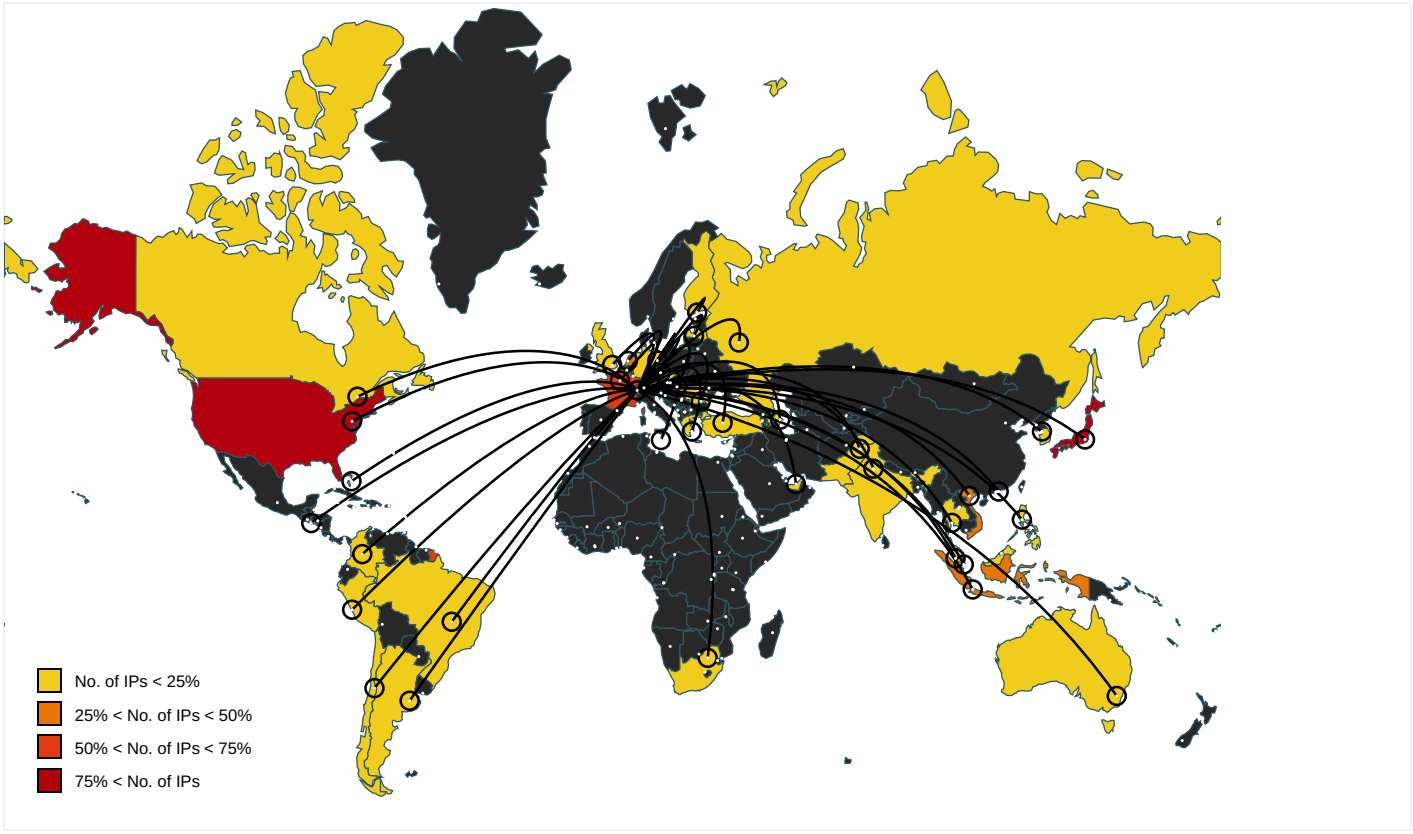
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://91.121.87.90:8080/KFDwQljVkxD3/OOFcmzcP5LKdqC/7kx60YXntHFlDt/5Rmtlx5Mir4E2nTGMFj/vs6RDbQfHrygTYrl/	true	• Avira URL Cloud: safe	unknown
http://177.130.51.198/43z7rPqPirmV4qB/AthcoPDmU/Q4ILc7kQKSHycUR/pIpU/8iSRPWx/wgrz9ygVvehFY9FxG0/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	certutil.exe, 00000002.0000000 2.2219887563.0000000002130000. 00000002.00000001.sdmp, tmp_e4 73b4.exe, 00000008.00000002.22 57462460.0000000002E50000.0000 0002.00000001.sdmp, normaliz.exe, 00000009.00000002.22616254 61.0000000003050000.00000002.0 0000001.sdmp, mmcshext.exe, 00 00000A.00000002.2265977899.000 0000002E80000.00000002.0000000 1.sdmp, ir50_qcx.exe, 0000000B .00000002.2270198814.000000000 2EF0000.00000002.00000001.sdmp, dhcpcmonitor.exe, 0000000C.0 0000002.2274808207.0000000002F 70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://pornthash.mobi/videos/tayna_tung	certutil.exe, 00000002.0000000 2.2220502859.0000000002600000. 00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	certutil.exe, 00000002.0000000 2.2219887563.0000000002130000. 00000002.00000001.sdmp, tmp_e4 73b4.exe, 00000008.00000002.22 57462460.0000000002E50000.0000 0002.00000001.sdmp, normaliz.exe, 00000009.00000002.22616254 61.0000000003050000.00000002.0 0000001.sdmp, mmcshext.exe, 00 00000A.00000002.2265977899.000 0000002E80000.00000002.0000000 1.sdmp, ir50_qcx.exe, 0000000B .00000002.2270198814.000000000 2EF0000.00000002.00000001.sdmp	false		high
http://https://pornthash.mobi/videos/tayna_tung%temp%/tmp_e473b4.exex	certutil.exe, 00000002.0000000 2.2220502859.0000000002600000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
126.126.139.26	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
203.153.216.178	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
104.131.144.215	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
143.95.101.72	unknown	United States		62729	ASMALLORANGE1US	true
162.144.145.58	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
180.23.53.200	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
190.164.135.81	unknown	Chile		22047	VTRBANDAANCHASACL	true
45.239.204.100	unknown	Brazil		268405	BMOBUENOCOMUNICACOES-MEBR	true
37.187.100.220	unknown	France		16276	OVHFR	true
190.85.46.52	unknown	Colombia		14080	TelmexColombiaSACO	true
88.247.58.26	unknown	Turkey		9121	TTNETTR	true
190.194.12.132	unknown	Argentina		10481	TelecomArgentinaSAAR	true
103.80.51.61	unknown	Thailand		136023	PTE-AS-APPTEGroupCoLtdTH	true
82.78.179.117	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
188.226.165.170	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
213.165.178.214	unknown	Malta		12709	MELITACABLEMT	true
119.92.77.17	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	true
46.105.131.68	unknown	France		16276	OVHFR	true
47.154.85.229	unknown	United States		5650	FRONTIER-FRTRUS	true
192.163.221.191	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
190.117.101.56	unknown	Peru		12252	AmericaMovilPeruSACPE	true
190.192.39.136	unknown	Argentina		10481	TelecomArgentinaSAAR	true
157.7.164.178	unknown	Japan		7506	INTERQGMOInternetIncJP	true
115.79.59.157	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
192.241.220.183	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
113.203.238.130	unknown	Pakistan		9387	AUGERE-PKAUGERE-PakistanPK	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.186.65.230	unknown	Turkey		9121	TTNETTR	true
46.32.229.152	unknown	United Kingdom		20738	GD-EMEA-DC-LD5GB	true
172.193.79.237	unknown	Australia		18747	IFX18747US	true
51.38.50.144	unknown	France		16276	OVHFR	true
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true
60.125.114.64	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
94.212.52.40	unknown	Netherlands		33915	TNF-ASNL	true
58.27.215.3	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	true
41.185.29.128	unknown	South Africa		36943	GridhostZA	true
91.75.75.46	unknown	United Arab Emirates		15802	DU-AS1AE	true
95.76.142.243	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	true
27.83.209.210	unknown	Japan		2516	KDDIKDDICORPORATIONJP	true
2.58.16.86	unknown	Latvia		64421	SERTEX-ASLV	true
221.147.142.214	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
188.166.220.180	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
115.79.195.246	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
118.33.121.37	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
188.40.170.197	unknown	Germany		24940	HETZNER-ASDE	true
179.5.118.12	unknown	El Salvador		14754	TelguaGT	true
36.91.44.183	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
192.210.217.94	unknown	United States		36352	AS-COLOCROSSINGUS	true
85.75.49.113	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	true
223.17.215.76	unknown	Hong Kong		18116	HGC-AS-APHGCGlobalCommunicationsLimitedHK	true
185.208.226.142	unknown	Hungary		43359	TARHELYHU	true
41.76.213.144	unknown	South Africa		37611	AfrihostZA	true
75.127.14.170	unknown	United States		36352	AS-COLOCROSSINGUS	true
172.96.190.154	unknown	Canada		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificptetldSG	true
91.121.87.90	unknown	France		16276	OVHFR	true
109.206.139.119	unknown	Russian Federation		47914	CDMSRU	true
103.229.73.17	unknown	Indonesia		55660	MWN-AS-IDPTMasterWebNetworkID	true
178.33.167.120	unknown	France		16276	OVHFR	true
43.255.175.197	unknown	Malaysia		9534	MAXIS-AS1-APBinariangBerhadMY	true
5.79.70.250	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true
120.51.34.254	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
125.200.20.233	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
103.93.220.182	unknown	Philippines		17639	CONVERGE-ASConvergeICTSolutionsIncPH	true
37.205.9.252	unknown	Czech Republic		24971	MASTER-ASCzechRepublicwwwmasterczCZ	true
118.243.83.70	unknown	Japan		4685	ASAHI-NETAsahiNetJP	true
172.105.78.244	unknown	United States		63949	LINODE-APLinodeLLCUS	true
123.216.134.52	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
91.213.106.100	unknown	Latvia		49667	IKFRIGA-ASLV	true
37.46.129.215	unknown	Russian Federation		29182	THEFIRST-ASRU	true
121.117.147.153	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.37.224.243	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	true
180.148.4.130	unknown	Viet Nam		45557	VNTT-AS-VNVietnamTechnologyandTelecommunicationJSCVN	true
113.161.148.81	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
116.202.10.123	unknown	Germany		24940	HETZNER-ASDE	true
177.130.51.198	unknown	Brazil		52747	WspServicosdeTelecomunicacoesLtdaBR	true
153.229.219.1	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
203.56.191.129	unknown	Australia		38220	AMAZE-SYD-AS-APwwwamazecomauAU	true
180.21.3.52	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
54.38.143.245	unknown	France		16276	OVHFR	true
77.74.78.80	unknown	Russian Federation		31261	GARS-ASMoscowRussiaRU	true
8.4.9.137	unknown	United States		3356	LEVEL3US	true
79.133.6.236	unknown	Finland		3238	ALCOMFI	true
202.29.237.113	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
185.80.172.199	unknown	Azerbaijan		39232	UNINETAZ	true
74.208.173.91	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
116.91.240.96	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
139.59.61.215	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
212.198.71.39	unknown	France		21502	ASN-NUMERICABLEFR	true
175.103.38.146	unknown	Indonesia		38320	MMS-AS-IDPTMaxindoMitraSolusiID	true
50.116.78.109	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
109.13.179.195	unknown	France		15557	LDCOMNETFR	true
42.200.96.63	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	true
73.100.19.104	unknown	United States		7922	COMCAST-7922US	true
24.231.51.190	unknown	Bahamas		15146	CABLEBAHAMASBS	true
190.151.5.131	unknown	Chile		6471	ENTELCHILESACL	true
113.193.239.51	unknown	India		45528	TIKONAIN-ASTikonaInfinetLtdIN	true
185.142.236.163	unknown	Netherlands		174	COGENT-174US	true
198.20.228.9	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
139.59.12.63	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
73.55.128.120	unknown	United States		7922	COMCAST-7922US	true
91.83.93.103	unknown	Hungary		12301	INVITECHHU	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	425356
Start date:	27.05.2021
Start time:	00:16:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
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:	18
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@0/100
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61.1% (good quality ratio 56.4%) • Quality average: 66.3% • Quality standard deviation: 27.6%
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
00:17:44	API Interceptor	226x Sleep call for process: svchost.exe modified
00:17:58	API Interceptor	10x Sleep call for process: tmp_e473b4.exe modified
00:18:01	API Interceptor	12x Sleep call for process: normaliz.exe modified
00:18:03	API Interceptor	11x Sleep call for process: mmcshext.exe modified
00:18:05	API Interceptor	11x Sleep call for process: ir50_qcx.exe modified
00:18:07	API Interceptor	11x Sleep call for process: dhcpcmonitor.exe modified
00:18:09	API Interceptor	10x Sleep call for process: adsmsext.exe modified
00:18:11	API Interceptor	11x Sleep call for process: TSChannel.exe modified
00:18:14	API Interceptor	8x Sleep call for process: qdvd.exe modified
00:18:16	API Interceptor	183x Sleep call for process: msvcp120_clr0400.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
126.126.139.26	MV9tCJw8Xr.exe	Get hash	malicious	Browse	
104.131.144.215	sample1.doc	Get hash	malicious	Browse	
	task5.doc	Get hash	malicious	Browse	
	P7Ya8tCZGu.exe	Get hash	malicious	Browse	
	http://asprise.com	Get hash	malicious	Browse	
	http://https://asprise.com	Get hash	malicious	Browse	
	A4Y5PZQuwQ.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E8ykSGwVtp.exe	Get hash	malicious	Browse	
	Pc3hLrhR6C.exe	Get hash	malicious	Browse	
	MzQN95jvoX.exe	Get hash	malicious	Browse	
	77CJzpSlkv.exe	Get hash	malicious	Browse	
	595Djs6jOC.exe	Get hash	malicious	Browse	
	AGWH4hi4Ig.exe	Get hash	malicious	Browse	
	1FFfIHDjlS.exe	Get hash	malicious	Browse	
	http://dentalalliance.se/wp-admin/public/SALhIWjtB/	Get hash	malicious	Browse	
	http://media.bolobedumusic.com/js/FILE/64576328218439519/IMOQa/	Get hash	malicious	Browse	
	http://https://fiera-deutzfahr.com/wp-admin/Overview/6555921/6uw9g10b-0079388/	Get hash	malicious	Browse	
143.95.101.72	Payment Advice Note ZRC-2020 (1).doc	Get hash	malicious	Browse	• 143.95.101.72:8080/Jto4JiPoOoGxpvR0u
203.153.216.178	MV9tCJw8Xr.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGAINFRASoftbankBBCorpJP	networkservice.exe	Get hash	malicious	Browse	• 126.242.192.104
	8UsA.sh	Get hash	malicious	Browse	• 60.139.247.213
	nT7K5GG5km	Get hash	malicious	Browse	• 220.49.0.51
	KnAY2OIPI3	Get hash	malicious	Browse	• 126.66.70.2
	ppc_unpacked	Get hash	malicious	Browse	• 60.98.164.138
	ldr.sh	Get hash	malicious	Browse	• 126.209.66.23
	rIbyGX66Op	Get hash	malicious	Browse	• 221.97.226.130
	MGuvcs6Ocz	Get hash	malicious	Browse	• 219.47.162.234
	IMG001.exe	Get hash	malicious	Browse	• 219.184.234.178
	YPJ9DZYIpO	Get hash	malicious	Browse	• 126.148.215.159
	KCCAfipQl2.dll	Get hash	malicious	Browse	• 49.253.193.36
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 60.108.128.186
	Io8ic2291n.doc	Get hash	malicious	Browse	• 60.93.23.51
	mozi.a.zip	Get hash	malicious	Browse	• 126.172.220.14
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 126.142.30.153
	WUHU95Apq3	Get hash	malicious	Browse	• 126.248.249.117
	bin.sh	Get hash	malicious	Browse	• 221.65.136.75
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 221.65.97.214
	mssecsvr.exe	Get hash	malicious	Browse	• 218.126.250.41
	mssecsvc.exe	Get hash	malicious	Browse	• 219.38.241.57
SURF-IDPTSurfindoNetworkID	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 203.153.216.189
	2ojdmC51As.exe	Get hash	malicious	Browse	• 203.153.216.189
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 203.153.216.178
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 203.153.216.189
	E0OuE7GkzY.exe	Get hash	malicious	Browse	• 203.153.216.182
	http://ehitusest.eu/marketplacel/sites/r5zmfubb2b/	Get hash	malicious	Browse	• 203.153.216.189
	_170105.exe	Get hash	malicious	Browse	• 203.153.216.182
	_170104.exe	Get hash	malicious	Browse	• 203.153.216.182
	_170106.exe	Get hash	malicious	Browse	• 203.153.216.182

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_170107.exe	Get hash	malicious	Browse	• 203.153.216.182
	_170103.exe	Get hash	malicious	Browse	• 203.153.216.182
	Inv_YKQG9770_181712165.doc	Get hash	malicious	Browse	• 203.153.216.182
	http://https://healinghandsonthemove.com/wp-content/2rugff7-99v83-292980/	Get hash	malicious	Browse	• 203.153.216.182
	Inv CKG36REGEX.doc	Get hash	malicious	Browse	• 203.153.216.182
	Estimativa J0370(1).doc	Get hash	malicious	Browse	• 203.153.216.182
	Invoice.doc	Get hash	malicious	Browse	• 203.153.216.182
	Estimativa.doc	Get hash	malicious	Browse	• 203.153.216.182
	FATURA(1).doc	Get hash	malicious	Browse	• 203.153.216.182
	Inv(3).doc	Get hash	malicious	Browse	• 203.153.216.182
	Estimate.doc	Get hash	malicious	Browse	• 203.153.216.182

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	
	sample1.doc	Get hash	malicious	Browse	
	sample1.doc	Get hash	malicious	Browse	
	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
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0002.doc	
Entropy (8bit):	3.9253267830463896
Encrypted:	false
SSDEEP:	12288:ade8HF9kUxyxlFnsn4yA9W8MZ5axhVYGByJGZGy9e3rfTqtTfLlR1xwSaf67HNu4:me8HFmU/4yA9W89VYU7sY7yz1DsVirpI
MD5:	DA122309698B26E96848A6A829EEF5C1
SHA1:	DFA1B8C96C19827A595EEB15B2EC5386F9746CEF
SHA-256:	26585F7107FBECBA9F5282D4C1F1783441C601870571331 21BD40D5C31C6149A
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. 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.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.A.E.A.A. A.A.D.A.B.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.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.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
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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//8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0291.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1191944
Entropy (8bit):	3.9253267830463896

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0291.doc	
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. 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.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.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\~WRD0416.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
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D50EB3E9-B04E-4308-B886-6463077025FE}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849456
Encrypted:	false
SSDEEP:	3:Iiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb5:IiiiiiiiifdLloZQc8++lsJe1MzKn
MD5:	9649F0A1F71A4D43EDD7A5BC31B8A43E
SHA1:	F2A1EBB9CD46A15DAB851068865C0EDA9A7B2CEC
SHA-256:	A815F7BE46CAC3CD990633D0DC3B30410858FA709DF4220AD8B33DB82AD3ED20
SHA-512:	9128C0D31E59E7870F15DA79BD166C478D29327A378DDF901B716B24A74A811743898ACEF6D81A298FF141A085A8A00F9864B88AB8D954785DDC4FC7F34BB358
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A.. ...."...&...*.......:...>... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F52B8A12-B174-499E-B3BD-E7523F18DF93}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F52B8A12-B174-499E-B3BD-E7523F18DF93}.tmp	
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
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 May 27 06:17:39 2021, mtime=Thu May 27 06:17:39 2021, atime=Thu May 27 06:17:41 2021, length=595972, window=hide
Category:	dropped
Size (bytes):	3660
Entropy (8bit):	4.4937442629551505
Encrypted:	false
SSDEEP:	96:8uk/XT+tyByK2uk/XT+tyByK2wk/XAt1O2wk/XAt12:8uwwu2uwwu2w/1pw/12
MD5:	0C0513DCA0BF6D1D9AFC673AFB880D3B
SHA1:	1A4DDA407197609DAC4A04465360A2B9F7680C5A
SHA-256:	5FA898CAD27FF5B3EF16C78FAD38B3CFD67A27847151A7498E16A24E3883EDB6
SHA-512:	FE0F4297CC442E9E755B6E681F36FE40FBCC0ABF7A61D6834178BABC64E0B0C8DBF60E4FE250861D39FEF00F2167E8A4CA86C2811529E5AE331827A5469468CD
Malicious:	false
Preview:	L.....F.... ....|.`.R...|.`.R...YLa.R.....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.....R5:..Public..b.....:...R5:*...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.....R5: .Ksh1.xls..>.....R4:.R4:*...,.... .....K.s.h.1.. .x.l.s.....k.....-...8...[.....?J.....C:\Users\..#.....\\376483\Users.Public\Ksh1.xls.!....\....\....\....\....\....\....\.P.u.b.l.i.c.\.K.s.h.1...x.l.s.....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.....376483..... ..D_....3N...W...9H.C.....[D_....3N...W...9H.C.....[....L.....F.... ....|.`.R...|.`.R...YLa.R.....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 May 27 06:17:39 2021, atime=Thu May 27 06:17:39 2021, length=4096, window=hide
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	4.470907538306087
Encrypted:	false
SSDEEP:	24:89p/XRlegvB3q6iL7Y2+G/XRlegvB3q6iL7c:8j/XjstfY2+G/Xjstfc
MD5:	B82B40CDE8C91EC708728BCAEB6ED185
SHA1:	73DEF80ECE7D0BF0DB7E208F1F3DBAA37EA7E30C
SHA-256:	A8EC0AFED648FDD1645D7A8603EA8DF354A7CE88C2473080425B516F6019B809
SHA-512:	6ACD2B9A72D586E263E2BED830AF542786454BCBA4DE48A787A991509AFF0ECB6FB90215DD2298558AED87C12373BDDB8D14251259B51A2996714B6AFE87521F
Malicious:	false
Preview:	L.....F.....1....|.`.R...|.`.R.....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\..#.....\\376483\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.....376483.....D_....3N...W...9G.C.....[D_....3N...W...9G.C.....[....L.....F.....1....Za.R.. .Za.R.....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 May 27 06:16:25 2021, mtime=Thu May 27 06:16:25 2021, atime=Thu May 27 06:16:31 2021, length=856064, window=hide
Category:	dropped
Size (bytes):	1994
Entropy (8bit):	4.503983456170819
Encrypted:	false
SSDEEP:	48:8Nm/XT0jDJQllhHDlOtQh2Nm/XT0jDJQllhHDlOtQ/:84/XojVtQh24/XojVtQ/
MD5:	D79CF64F781B213CE72965233760B911
SHA1:	0EC073D030B6690CD751F9B6F07371F92ECF7077
SHA-256:	205B59476CA151EB3DBC738D47447A7E7CD0E293F3FB56572B7A9B87F2EACE34
SHA-512:	870D1D8140863E81B652685647A97E9DCF7867518D2367BDC8B04D8930E734D8CAE592DC810A22BBA28E79C54657B047DBC3324ABE265313AF25DBC72FB6B73
Malicious:	false
Preview:	L.....F.... .....4.R.....4.R.....7.R.....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.:*...0&.....s.a.m.p.l.e.1...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\376483\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.....376483.....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
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:vdsCkWtW2IIID9l
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

C:\Users\Public\Ksh1.pdf	
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 41%, Browse • Antivirus: ReversingLabs, Detection: 67%
Joe Sandbox View:	• Filename: sample1.doc, Detection: malicious, Browse • Filename: sample1.doc, Detection: malicious, Browse • 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.d W..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:vdsCkWtW2IIID9l
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:vdsCkWtW2IIID9l
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\~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:	56B3941CD93658F7DF8976213E2DFD5CB74E7ABB651AD26FDA9B7191E675E03289366B32EEDF68D139562A88DBBAE2589FDA8ABBDB756C43E2E605863459A162
Malicious:	false

C:\Users\Public\~WRD0000.tmp	
Preview:	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACAEAAA4fug4AtAnNIbgBTM0hVGhpcy Bwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAApTiijbS9G8G0vRvBtL0bw2bO38GcvRvDZs7XwGi9G8NmztPB1L0bwP0dD8U 0vRvA/R0LxYi9G8D9HRfF+L0bwZFfV8GgvRvBtL0fwCS9G8PdGT/FsL0bw90ZG8WwvRvD3RrnwbC9G8G0v0fBsL0bw90ZE8WwvRvBSaWNobS9G8AAAAAAAAAA AAUEUAAEwBBQAr7ZhfAAAAAAAAAAAADgAAIhCwEOEAAUAQAAxAUAAAAAAAGR9AAAAEAAAADABAAAAABAAEAAAAAIAAAUAAQAAAAAABQABAAAAAAAA EAcAAAQAAAAAAAAADAEABAAAQAAAQAAAAABAAABAAAAAAAAAAQAAAAEIUBAEgAAABYhQEAPAAAAACwAQBQQgUAAAAAAAAAAAAAAAAAAAAAAAAABw CIDgAAMHwBADgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABofAEAQAAAAAAAAAAAAAAAAADABADgBAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAudGV4dAAAAGcSAQAAEAAAABQBAAAEAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAABkXAAAADABAABeAAAAGAEAAAAAAAAAAAAAAAAAAQAAAQC 5kYXRhAAAA6BEAAACQAQAACAAAAHYBAAAAAAAAAAAAAAAAAAEAAAMAucnNyYwAAAFBCBQAAsAEAAEQFAAB+AQAAAAAAAAAAAAAAAAABAAABALnJl bG9jAACIDgAAAAAHAAAQAAAAwgYAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

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 Pag es: 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:	dc40e48d2eb0e57cd16b1792bdccc185440f632783c7bc c87c955e1d4e88fc95
SHA512:	a851ac80b43ebdb8e990c2eb3daabb456516fc40bb43c9f 76d0112674dbd6264efce881520744f0502f2962fc0bb40 24e7d73ea66d56bc87c0cc6dfde2ab869a
SSDEEP:	12288:emkTbAui+yjlKtAMgWffRtpqgnydr6YqVPCspBZ ZLFLIx/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
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 . .

General	
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 00 00 00 53 6c 65 70 00 00 00 00 ff ff ff ff 01 00 00 00 ff 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
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 . . . Microsoft Word 97-2003 Document . . . . . MSWordDoc . . . . . Word.Document.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
File Type:	data
Stream Size:	7386
Entropy:	5.92077573609
Base64 Encoded:	True
Data ASCII:	. . . . . x . . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 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 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 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 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
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

General	
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 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 00 00 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

Network Port Distribution

Total Packets: 13

- 8080 undefined
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 00:19:05.781451941 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.090272903 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.090476036 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.091706991 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.091789961 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.399941921 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.400216103 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.400232077 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.400314093 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:06.707856894 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.708199978 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.708224058 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.709530115 CEST	80	49172	177.130.51.198	192.168.2.22
May 27, 2021 00:19:06.709599972 CEST	49172	80	192.168.2.22	177.130.51.198
May 27, 2021 00:19:07.067719936 CEST	49173	8080	192.168.2.22	91.121.87.90
May 27, 2021 00:19:07.121426105 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.121526957 CEST	49173	8080	192.168.2.22	91.121.87.90
May 27, 2021 00:19:07.122493982 CEST	49173	8080	192.168.2.22	91.121.87.90
May 27, 2021 00:19:07.122662067 CEST	49173	8080	192.168.2.22	91.121.87.90
May 27, 2021 00:19:07.176059008 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.176095963 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.176537037 CEST	49173	8080	192.168.2.22	91.121.87.90
May 27, 2021 00:19:07.228121042 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.228171110 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.228199005 CEST	8080	49173	91.121.87.90	192.168.2.22
May 27, 2021 00:19:07.228286028 CEST	49173	8080	192.168.2.22	91.121.87.90

HTTP Request Dependency Graph

- 177.130.51.198
- 91.121.87.90
  - 91.121.87.90:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49172	177.130.51.198	80	C:\Windows\SysWOW64\whhelper\msvcp120_clr0400.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2021 00:19:06.091706991 CEST	11157	OUT	POST /43z7rPqPirmV4qB/AthcoPDmU/Q4ILc7kQKSHycUR/pIpU/8iSRPWx/wgrz9ygVvehFY9FxG0/ HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate DNT: 1 Connection: keep-alive Referer: 177.130.51.198/ Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=----------fZX6grGG67bSvix2bq9 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: 177.130.51.198 Content-Length: 4452 Cache-Control: no-cache
May 27, 2021 00:19:06.709530115 CEST	11162	IN	HTTP/1.1 400 Bad Request Date: Wed, 26 May 2021 23:19:05 GMT Server: Boa/0.94.13 Content-Type: text/html; charset=ISO-8859-1 Content-Length: 151 Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 3e 3c 48 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 48 31 3e 0a 59 6f 75 72 20 63 6c 69 65 6e 74 20 68 61 73 20 69 73 73 75 65 64 20 61 20 6d 61 6c 66 6f 72 6d 65 64 20 6f 72 20 69 6c 6c 65 67 61 6c 20 72 65 71 75 65 73 74 2e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a Data Ascii: <HTML><HEAD><TITLE>400 Bad Request</TITLE></HEAD><BODY><H1>400 Bad Request</H1>Your client has issued a malformed or illegal request.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49173	91.121.87.90	8080	C:\Windows\SysWOW64\whhelper\msvcp120_clr0400.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2021 00:19:07.122493982 CEST	11163	OUT	POST /KFDwQljVkxD3/OOFcmzcP5LKdqC/7kx60YXntHFlDt/5Rmtlx5Mir4E2nTGMFj/vs6RDbQfHrygTYrl/ HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate DNT: 1 Connection: keep-alive Referer: 91.121.87.90/ Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=----------F6CkwVxliFrUl7pi 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: 91.121.87.90:8080 Content-Length: 4452 Cache-Control: no-cache
May 27, 2021 00:19:07.228199005 CEST	11168	IN	HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Wed, 26 May 2021 22:19:07 GMT Content-Length: 19 Data Raw: 34 30 34 20 70 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 0a Data Ascii: 404 page not found

Code Manipulations

Statistics

Behavior

- WINWORD.EXE
- certutil.exe
- svchost.exe
- tmp_e473b4.exe
- normaliz.exe
- mmcshext.exe
- ir50_qcx.exe
- dhcpcmonitor.exe
- adsmsext.exe
- TSChannel.exe
- qdvd.exe
- msvcp120_clr0400.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1492 Parent PID: 584

General

Start time:	00:16:31
Start date:	27/05/2021
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:	0x13f120000
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\~DF41535F9E547D22F9.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\F2EFC	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\F2EFC	F2EFC	binary	04 00 00 00 D4 05 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 F9 30 89 4A C8 52 D7 01 FC 2E 0F 00 FC 2E 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	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 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	1387986990	1387986991	success or wait	1	7FEE90A9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1387986991	1387986992	success or wait	1	7FEE90A9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F2EFC	F2EFC	binary	04 00 00 00 D4 05 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	04 00 00 00 D4 05 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	success or wait	1	7FEE90A9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			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 F9 30 89 4A C8 52 D7 01 FC 2E 0F 00 FC 2E 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 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 FC 2E 0F 00 FC 2E 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				

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 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 FF FF FF FF				

Analysis Process: certutil.exe PID: 2336 Parent PID: 1220

General

Start time:	00:17:42
Start date:	27/05/2021
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	Certutil -decode C:\Users\Public\Ksh1.xls C:\Users\Public\Ksh1.pdf
Imagebase:	0xffa70000
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\cer69EA.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	FFB21B04	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\cer69EA.tmp	success or wait	1	FFB21B34	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: 2904 Parent PID: 428

General

Start time:	00:17:43
Start date:	27/05/2021
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: 1872 Parent PID: 3040

General

Start time:	00:17:56
Start date:	27/05/2021
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: 00000008.00000002.2255546226.0000000000641000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000002.2255733615.0000000000926000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000008.00000003.2251551044.0000000000928000.00000004.00000001.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: normaliz.exe PID: 2400 Parent PID: 1872

General

Start time:	00:17:59
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\mfcm140\normaliz.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mfcm140\normaliz.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: 00000009.00000002.2260946472.00000000003F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000003.2256075266.0000000000658000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.2261089149.0000000000614000.00000004.00000020.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: mmcshext.exe PID: 2496 Parent PID: 2400

General

Start time:	00:18:01
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\clip\mmcshext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\clip\mmcshext.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.00000003.2260910791.0000000000688000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2265106835.00000000003F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000A.00000002.2265371977.0000000000686000.00000004.00000020.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: ir50_qcx.exe PID: 2104 Parent PID: 2496

General

Start time:	00:18:03
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\regedt32\ir50_qcx.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regedt32\ir50_qcx.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.00000002.2269436388.0000000000331000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000002.2269524139.0000000000504000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000B.00000003.2265408389.0000000000548000.00000004.00000001.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: dhcpcmonitor.exe PID: 2552 Parent PID: 2104

General

Start time:	00:18:05
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\KBDNEPR\dhcpcmonitor.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\KBDNEPR\dhcpcmonitor.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.00000002.2274011391.00000000004F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.2273841914.00000000002F6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000003.2269934201.00000000002F8000.00000004.00000001.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: adsmsext.exe PID: 1616 Parent PID: 2552

General

Start time:	00:18:07
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\api-ms-win-core-interlocked-l1-1-0\adsmsext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\api-ms-win-core-interlocked-l1-1-0\adsmsext.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.00000003.2274679265.00000000005B8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2278477954.0000000000574000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000D.00000002.2278304115.0000000000291000.00000020.00000001.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: TSChannel.exe PID: 2856 Parent PID: 1616

General

Start time:	00:18:09
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\oleaccrc\TSChannel.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\oleaccrc\TSChannel.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.00000003.2279155029.00000000002B8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2282904583.0000000000274000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000E.00000002.2286207050.0000000001C61000.00000020.00000001.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: qdvd.exe PID: 2748 Parent PID: 2856

General

Start time:	00:18:12
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\iprtrmgr\qdvd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\iprtrmgr\qdvd.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.00000002.2289663022.00000000005B6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000003.2284287661.00000000005B8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000F.00000002.2289418364.00000000003F1000.00000020.00000001.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: msvcp120_clr0400.exe PID: 1036 Parent PID: 2748

General

Start time:	00:18:14
Start date:	27/05/2021
Path:	C:\Windows\SysWOW64\whhelper\msvcp120_clr0400.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\whhelper\msvcp120_clr0400.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: 00000010.00000002.2330396700.00000000002B4000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000002.2330617776.0000000000471000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000010.00000003.2289619290.00000000002F8000.00000004.00000001.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	472FB8	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	472FB8	HttpSendRequestW
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	472FB8	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	472FB8	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	472FB8	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	472FB8	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	472FB8	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	472FB8	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	472FB8	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