ID: 778230
Sample Name:
KuponcuBaba.exe
Cookbook: default.jbs
Time: 08:54:13
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

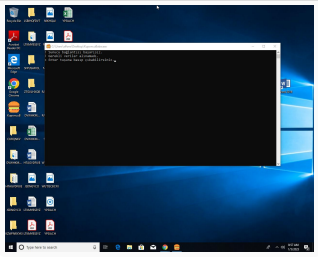
Windows Analysis Report

KuponcuBaba.exe

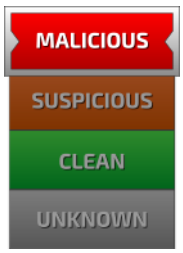
Overview

General Information

Sample Name:	KuponcuBaba.exe
Analysis ID:	778230
MD5:	d6c3bf64cc7cb1…
SHA1:	2ea0b0bda586ae.
SHA256:	d91890315262e8.
Tags:	exe
Infos:	



Detection

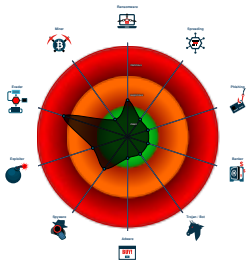


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Hides threads from debuggers
- Contains functionality to infect the b…
- Modifies the context of a thread in a…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Sample execution stops while proce…
- Contains functionality to communica…

Classification



Process Tree

- **System is w10x64**
- KuponcuBaba.exe (PID: 2820 cmdline: C:\Users\user\Desktop\KuponcuBaba.exe MD5: D6C3BF64CC7CB131D467246CE5A4C455)
  - conhost.exe (PID: 64 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - KuponcuBaba.exe (PID: 5192 cmdline: C:\Users\user\Desktop\KuponcuBaba.exe MD5: D6C3BF64CC7CB131D467246CE5A4C455)
    - cmd.exe (PID: 2772 cmdline: C:\Windows\system32\cmd.exe /c "ver" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - cmd.exe (PID: 5416 cmdline: C:\Windows\system32\cmd.exe /c @echo off MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - cmd.exe (PID: 5540 cmdline: C:\Windows\system32\cmd.exe /c cls MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Persistence and Installation Behavior

Contains functionality to infect the boot sector

Boot Survival

Contains functionality to infect the boot sector

Anti Debugging

Hides threads from debuggers

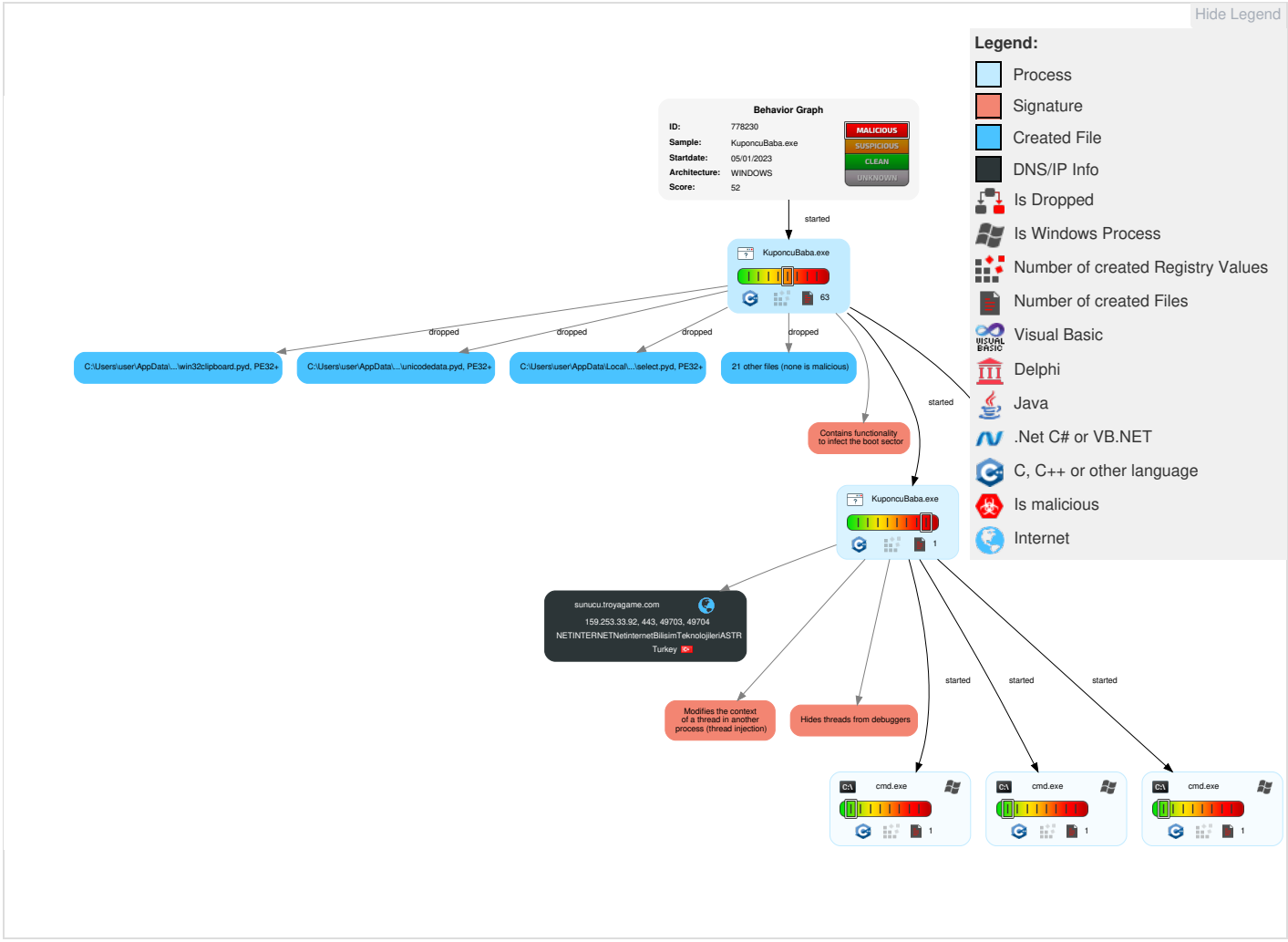
HIPS / PFW / Operating System Protection Evasion

Modifies the context of a thread in another process (thread injection)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Bootkit	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 1 Process Injection	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Bootkit	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

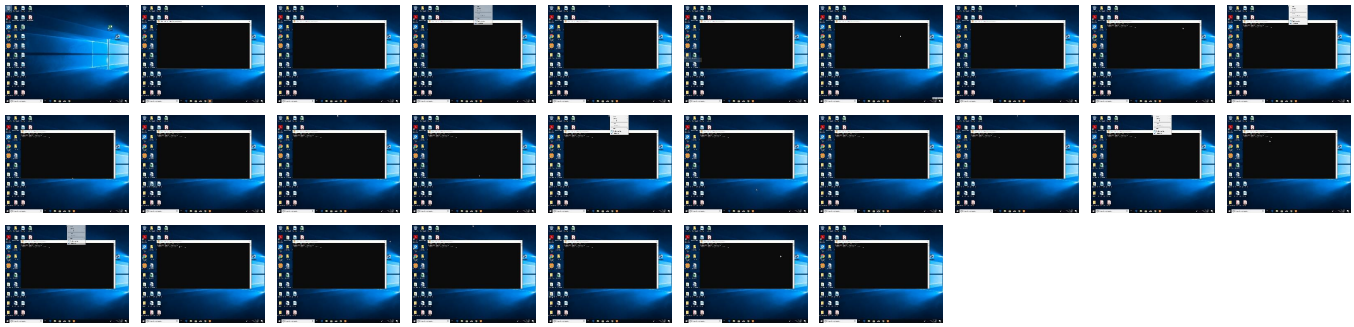
Behavior Graph



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
KuponcuBaba.exe	2%	ReversingLabs		
KuponcuBaba.exe	6%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp_MEI28202\VCRUNTIME140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_bz2.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_cffi_backend.cp310-win_amd64.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_ctypes.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_decimal.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_hashlib.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_lzma.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_pytransform.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_queue.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_socket.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_ssl.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202_uuid.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\cryptography\hazmat\bindings_openssl.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\cryptography\hazmat\bindings_rust.pyd	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp_MEI28202\libcrypto-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\libffi-7.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\libssl-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\pyexpat.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\python3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\python310.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\pywintypes310.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\select.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\unicodedata.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp_MEI28202\win32clipboard.pyd	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sunucu.troyagame.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.dhimyotis.com/certignarootca.crl	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl	0%	URL Reputation	safe	
http://127.0.0.1:4444/wd/hub	1%	Virustotal		Browse
http://https://sunucu.troyagame.com/	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl3.digi	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://127.0.0.1:4444/wd/hub	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/html/sec-forms.html#multipart-form-data	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://127.0.0.1:%s/status	0%	Avira URL Cloud	safe	
http://ocsp.accv.esPE	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#dfn-insecure-tls-certificates	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/STCA.crlr	0%	Avira URL Cloud	safe	
http://https://www.selenium.dev/downloads/	0%	Avira URL Cloud	safe	
http://crl3.digiz	0%	Avira URL Cloud	safe	
http://https://wwww.certigna.fr/autorites/s	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#dfn-browser-version	0%	Avira URL Cloud	safe	
http://127.0.0.1:4444	0%	Avira URL Cloud	safe	
http://.../back.jpeg	0%	Avira URL Cloud	safe	
http://https://mahler:8092/site-updates.py	0%	Avira URL Cloud	safe	
http://https://chromedevtools.github.io/devtools-protocol/	0%	Avira URL Cloud	safe	
http://sunucu.troyagame.com/z	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#timeouts	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#dfn-strict-file-interactability	0%	Avira URL Cloud	safe	
http://sunucu.troyagame.com/	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#dfn-platform-name	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl_	0%	Avira URL Cloud	safe	
http://https://w3c.github.io/webdriver/#dfn-table-of-page-load-strategies	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sunucu.troyagame.com	159.253.33.92	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sunucu.troyagame.com/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/SeleniumHQ/selenium/wiki/JsonWireProtocol)	KuponcuBaba.exe, 00000007.00000002.56475 0127.0000027F050A4000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://https://cloud.google.com/appengine/docs/standard/runtimes	KuponcuBaba.exe, 00000007.00000002.56169 9929.0000027F04930000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://crl3.digiz	KuponcuBaba.exe, 00000001.00000003.29209 6227.000001A41CE34000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/mhammond/pywin32	KuponcuBaba.exe, 00000001.00000003.29569 0492.000001A41CE37000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000001.00000003.295672850.000001A41CE 2A000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000001.000000 03.294934339.000001A41CE29000.00000004.0 0000020.00020000.00000000.sdmp, KuponcuB aba.exe, 00000007.00000002.572718758.000 07FFA0AC62000.00000002.00000001.01000000 .00000017.sdmp, KuponcuBaba.exe, 0000000 7.00000002.573581346.00007FFA18E38000.00 000002.00000001.01000000.00000016.sdmp	false		high
http://pypi.python.org/pypi/wget/	KuponcuBaba.exe, 00000007.00000002.56270 7463.0000027F04B59000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://python.org/dev/peps/pep-0263/	KuponcuBaba.exe, 00000007.00000002.57158 2077.00007FFA06D5E000.00000002.00000001. 01000000.00000005.sdmp	false		high
http://https://github.com/tensorflow/datasets/blob/master/tensorflow_datasets/core/utils/resource_utils.py#	KuponcuBaba.exe, 00000007.00000002.55700 6907.0000027F022D1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300075577.0000027F022 D1000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 03.300234894.0000027F022D1000.00000004.0 0000020.00020000.00000000.sdmp, KuponcuB aba.exe, 00000007.00000003.299922007.000 0027F022F9000.00000004.00000020.00020000 .00000000.sdmp, KuponcuBaba.exe, 0000000 7.00000003.299928153.0000027F022A7000.00 000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.30017 0147.0000027F022D1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.556629333.0000027F022 5D000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 03.300206686.0000027F022A5000.00000004.0 0000020.00020000.00000000.sdmp	false		high
http://127.0.0.1:4444/wd/hub	KuponcuBaba.exe, 00000007.00000002.55865 0240.0000027F029A0000.00000004.00000020. 00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://bitbucket.org/techtonik/python-pager	KuponcuBaba.exe, 00000007.00000002.56454 6201.0000027F05060000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://https://github.com/pyca/cryptography/actions?query=workflow%3ACI	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://tools.ietf.org/html/rfc2388#section-4.4	KuponcuBaba.exe, 00000007.00000002.55973 0683.0000027F04430000.00000004.00000020. 00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.apache.org/licenses/LICENSE-2.0	KuponcuBaba.exe, 00000001.00000003.29689 1487.000001A41CE39000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000001.00000003.296719687.000001A41CE 2A000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000001.000000 03.296737570.000001A41CE38000.00000004.0 0000020.00020000.00000000.sdmp, LICENSE. APACHE.1.dr	false		high
http://https://www.yemeksepeti.com/	KuponcuBaba.exe, 00000007.00000002.56057 1375.0000027F04630000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://https://sunucu.troyagame.com/	KuponcuBaba.exe, 00000007.00000002.56589 4975.0000027F051F4000.00000004.00001000. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.564546201.0000027F050 60000.00000004.00001000.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 02.560325416.0000027F045BB000.00000004.0 0000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.swisssign.com/(IK	KuponcuBaba.exe, 00000007.00000002.56317 6497.0000027F04C39000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://www.selenium.dev/downloads/	KuponcuBaba.exe, 00000007.00000002.55700 6907.0000027F022D1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.564750127.0000027F050 A4000.00000004.00001000.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl	KuponcuBaba.exe, 00000007.00000002.56350 7590.0000027F04CC1000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://curl.haxx.se/rfc/cookie_spec.html	KuponcuBaba.exe, 00000007.00000002.56212 3971.0000027F04A30000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://ocsp.accv.es	KuponcuBaba.exe, 00000007.00000002.56330 0269.0000027F04C6E000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://w3c.github.io/webdriver/#dfn-browser-version	KuponcuBaba.exe, 00000007.00000002.56212 3971.0000027F04A30000.00000004.00001000. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://json.org	KuponcuBaba.exe, 00000007.00000002.55865 0240.0000027F029A0000.00000004.00000020. 00020000.00000000.sdmp	false		high
http:// https://github.com/python/cpython/blob/3.9/Lib/importlib/_bootstrap_external.py#L679-L688	KuponcuBaba.exe, 00000007.00000003.29996 8567.0000027F022F8000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.557606845.0000027F026 E8000.00000004.00001000.00020000.0000000 0.sdmp	false		high
http://https://httpbin.org/get	KuponcuBaba.exe, 00000007.00000002.56449 3371.0000027F05050000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://https://w3c.github.io/webdriver/#dfn-insecure-tls-certificates	KuponcuBaba.exe, 00000007.00000002.56438 5194.0000027F05030000.00000004.00001000. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://httpbin.org/	KuponcuBaba.exe, 00000007.00000002.55700 6907.0000027F022D1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.334518018.0000027F045 CD000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 02.560325416.0000027F045BB000.00000004.0 0000020.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	KuponcuBaba.exe, 00000007.00000002.56350 7590.0000027F04CC1000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/python/cpython/blob/839d7893943782ee803536a47f1d4de160314f85/Lib/importlib/reader	KuponcuBaba.exe, 00000007.00000002.5570006907.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300075577.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300234894.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.299922007.0000027F022F9000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.299928153.0000027F022A7000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300170147.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.556629333.0000027F0225D000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300206686.0000027F022A5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://httpbin.org/	KuponcuBaba.exe, 00000007.00000002.5570006907.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.334518018.0000027F045CD000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.560325416.0000027F045BB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.apache.org/licenses/	KuponcuBaba.exe, 00000001.00000003.296719687.000001A41CE2A000.00000004.00000020.00020000.00000000.sdmp, LICENSE.APACHE.1.dr	false		high
http://https://github.com/pyca/cryptography/workflows/CI/badge.svg?branch=main	KuponcuBaba.exe, 00000001.00000003.297191026.000001A41CE2D000.00000004.00000020.00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://wwww.certigna.fr/autorites/	KuponcuBaba.exe, 00000007.00000002.563507590.0000027F04CC1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/SeleniumHQ/selenium/wiki/DesiredCapabilities	KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.562815618.0000027F04B94000.00000004.00000020.00020000.00000000.sdmp	false		high
http://127.0.0.1:%s/status	KuponcuBaba.exe, 00000007.00000002.564750127.0000027F050A4000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://hg.python.org/cpython/file/603b4d593758/Lib/socket.py#l535	KuponcuBaba.exe, 00000007.00000002.5570006907.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cryptography.io/en/latest/installation/	KuponcuBaba.exe, 00000001.00000003.297191026.000001A41CE2D000.00000004.00000020.00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://github.com/Unidata/MetPy/blob/a3424de66a44bf3a92b0dcacf4dff82ad7b86712/src/metpy/plots/wx_sy	KuponcuBaba.exe, 00000007.00000002.5570006907.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300075577.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300234894.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.299922007.0000027F022F9000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.299928153.0000027F022A7000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300170147.0000027F022D1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.556629333.0000027F0225D000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300206686.0000027F022A5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.securetrust.com/STCA.crlr	KuponcuBaba.exe, 00000007.00000002.560416129.0000027F045F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	KuponcuBaba.exe, 00000007.00000002.563300269.0000027F04C6E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.securetrust.com/STCA.crl	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://chromedriver.chromium.org/home	KuponcuBaba.exe, 00000007.00000002.56475 0127.0000027F050A4000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://wwwsearch.sf.net/):	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	KuponcuBaba.exe, 00000007.00000002.56330 0269.0000027F04C6E000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.accv.es/legislacion_c.htm	KuponcuBaba.exe, 00000007.00000002.56317 6497.0000027F04C39000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://tools.ietf.org/html/rfc6125#section-6.4.3	KuponcuBaba.exe, 00000007.00000002.56169 9929.0000027F04930000.00000004.00001000. 00020000.00000000.sdmp	false		high
http://https://cryptography.io/en/latest/security/	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://cffi.readthedocs.io/en/latest/using.html#callbacks	_cffi_backend.cp310-win_amd64.pyd.1.dr	false		high
http://crl.xrampsecurity.com/XGCA.crl0	KuponcuBaba.exe, 00000007.00000002.56032 5416.0000027F045BB000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.cert.fnmt.es/dpcs/	KuponcuBaba.exe, 00000007.00000002.56330 0269.0000027F04C6E000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://www.yemeksepeti.com/rj	KuponcuBaba.exe, 00000007.00000002.55973 0683.0000027F04430000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.558650240.0000027F029 A0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.562815618.0000027F04B 94000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	KuponcuBaba.exe, 00000007.00000002.56317 6497.0000027F04C39000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.563300269.0000027F04C 6E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/python/cpython/blob/839d7893943782ee803536a47f1d4de160314f85/Lib/importlib/abc.py	KuponcuBaba.exe, 00000007.00000003.30020 6686.0000027F022A5000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/s	KuponcuBaba.exe, 00000007.00000002.56350 7590.0000027F04CC1000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/pyca/cryptography/issues	METADATA.1.dr	false		high
http://https://readthedocs.org/projects/cryptography/badge/?version=latest	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://ocsp.accv.esPE	KuponcuBaba.exe, 00000007.00000002.56330 0269.0000027F04C6E000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://google.com/	KuponcuBaba.exe, 00000007.00000002.56032 5416.0000027F045BB000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://mahler:8092/site-updates.py	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://127.0.0.1:4444	KuponcuBaba.exe, 00000007.00000002.56463 1005.0000027F05078000.00000004.00001000. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/SeleniumHQ/selenium/wiki/JsonWireProtocol	KuponcuBaba.exe, 00000007.00000002.563722039.0000027F04F30000.00000004.00001000.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.561089027.0000027F04830000.00000004.00001000.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.564546201.0000027F05060000.00000004.00001000.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.562815618.0000027F04B94000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.564750127.0000027F050A4000.00000004.00001000.00020000.00000000.sdmp	false		high
http://.../back.jpeg	KuponcuBaba.exe, 00000007.00000002.562123971.0000027F04A30000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/pyca/cryptography	KuponcuBaba.exe, 00000001.00000003.297191026.000001A41CE2D000.00000004.00000020.00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://www.python.org/download/releases/2.3/mro/.	KuponcuBaba.exe, 00000007.00000002.557187866.0000027F02660000.00000004.00001000.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.300707340.0000027F029DA000.00000004.00000020.00020000.00000000.sdmp, base_library.zip.1.dr	false		high
http://https://cryptography.io/	METADATA.1.dr	false		high
http://https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#https-proxy-error-http-proxy	KuponcuBaba.exe, 00000007.00000002.560571375.0000027F04630000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://httpbin.org/post	KuponcuBaba.exe, 00000007.00000003.333554896.0000027F02A48000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.559160943.0000027F02A67000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://chromedevtools.github.io/devtools-protocol/	KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/pyca/cryptography/	KuponcuBaba.exe, 00000001.00000003.297191026.000001A41CE2D000.00000004.00000020.00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://github.com/Ousret/charset_normalizer	KuponcuBaba.exe, 00000007.00000002.560325416.0000027F045BB000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/urllib3/urllib3/issues/497	KuponcuBaba.exe, 00000007.00000002.561089027.0000027F04830000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	KuponcuBaba.exe, 00000007.00000002.563176497.0000027F04C39000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.563507590.0000027F04CC1000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.563280811.0000027F04C6B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://bitbucket.org/techtonik/python-wget/	KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.securetrust.com/SGCA.crl0	KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl3.digi	KuponcuBaba.exe, 00000001.00000003.292096227.000001A41CE34000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	KuponcuBaba.exe, 00000007.00000002.562707463.0000027F04B59000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://w3c.github.io/webdriver/#timeouts	KuponcuBaba.exe, 00000007.00000002.564750127.0000027F050A4000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://codecov.io/github/pyca/cryptography/coverage.svg?branch=main	KuponcuBaba.exe, 00000001.00000003.297191026.000001A41CE2D000.00000004.00000020.00020000.00000000.sdmp, METADATA.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://yahoo.com/	KuponcuBaba.exe, 00000007.00000002.55700 6907.0000027F022D1000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.560325416.0000027F045 BB000.00000004.00000020.00020000.0000000 0.sdmp	false		high
http://https://w3c.github.io/webdriver/#dfn-platform-name	KuponcuBaba.exe, 00000007.00000002.56454 6201.0000027F05060000.00000004.00001000. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-6	KuponcuBaba.exe, 00000007.00000003.33406 0970.0000027F044A6000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.560131047.0000027F045 06000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 03.333732076.0000027F04506000.00000004.0 0000020.00020000.00000000.sdmp, KuponcuB aba.exe, 00000007.00000003.333894641.000 0027F04507000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	KuponcuBaba.exe, 00000001.00000003.29276 0666.000001A41CE29000.00000004.00000020. 00020000.00000000.sdmp, libffi-7.dll.1.dr	false		high
http://https://w3c.github.io/html/sec-forms.html#multipart-form-data	KuponcuBaba.exe, 00000007.00000002.55865 0240.0000027F029A0000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps0	KuponcuBaba.exe, 00000007.00000002.56317 6497.0000027F04C39000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl	KuponcuBaba.exe, 00000007.00000002.56317 6497.0000027F04C39000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0	KuponcuBaba.exe, 00000007.00000002.56330 0269.0000027F04C6E000.00000004.00000020. 00020000.00000000.sdmp	false		high
http://https://cryptography.io/en/latest/changelog/	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://mail.python.org/mailman/listinfo/cryptography-dev	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://codecov.io/github/pyca/cryptography?branch=main	KuponcuBaba.exe, 00000001.00000003.29719 1026.000001A41CE2D000.00000004.00000020. 00020000.00000000.sdmp, METADATA.1.dr	false		high
http://https://requests.readthedocs.io	KuponcuBaba.exe, 00000007.00000002.56372 2039.0000027F04F30000.00000004.00001000. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000003.333554896.0000027F02A 48000.00000004.00000020.00020000.0000000 0.sdmp, KuponcuBaba.exe, 00000007.000000 02.559160943.0000027F02A67000.00000004.0 0000020.00020000.00000000.sdmp	false		high
http://repository.swisssign.com/	KuponcuBaba.exe, 00000007.00000002.56292 6496.0000027F04BD2000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.563176497.0000027F04C 39000.00000004.00000020.00020000.0000000 0.sdmp	false		high
http://https://w3c.github.io/webdriver/#dfn-strict-file-interactability	KuponcuBaba.exe, 00000007.00000002.56212 3971.0000027F04A30000.00000004.00001000. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://w3c.github.io/webdriver/#dfn-table-of-page-load-strategies	KuponcuBaba.exe, 00000007.00000002.56372 2039.0000027F04F30000.00000004.00001000. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.564385194.0000027F050 30000.00000004.00001000.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl	KuponcuBaba.exe, 00000007.00000002.56041 6129.0000027F045F1000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	KuponcuBaba.exe, 00000001.00000003.29801 5876.000001A41CE2E000.00000004.00000020. 00020000.00000000.sdmp, KuponcuBaba.exe, 00000001.00000003.298020453.000001A41CE 30000.00000004.00000020.00020000.0000000 0.sdmp, mutation-listener.js.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sunucu.troyagame.com/z	KuponcuBaba.exe, 00000007.00000002.559730683.0000027F04430000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.558650240.0000027F029A0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.python.org	KuponcuBaba.exe, 00000007.00000003.333554896.0000027F02A48000.00000004.00000020.00020000.00000000.sdmp, KuponcuBaba.exe, 00000007.00000002.559160943.0000027F02A67000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.accv.es/legislacion_c.htm0U	KuponcuBaba.exe, 00000007.00000002.563300269.0000027F04C6E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.securetrust.com/SGCA.crl_	KuponcuBaba.exe, 00000007.00000002.560416129.0000027F045F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
159.253.33.92	sunucu.troyagame.com	Turkey		51559	NETINTERNETNetinternet BilisimTeknolojileriASTR	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778230
Start date and time:	2023-01-05 08:54:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KuponcuBaba.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	mal52.evad.winEXE@10/40@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp_MEI28202\VCRUNTIME140.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	97168
Entropy (8bit):	6.424686954579329
Encrypted:	false
SSDEEP:	1536:yKHLG4SsAzAvadZw+1Hcx8uIYNUzU6Ha4aecbK/zJZ0/b:yKrfZ+jPYNz6Ha4aecbK/FZK
MD5:	A87575E7CF8967E481241F13940EE4F7
SHA1:	879098B8A353A39E16C79E6479195D43CE98629E
SHA-256:	DED5ADAA94341E6C62AEA03845762591666381DCA30EB7C17261DD154121B83E
SHA-512:	E112F267AE4C9A592D0DD2A19B50187EB13E25F23DED74C2E6CCDE458BCDAEE99F4E3E0A00BAF0E3362167AE7B7FE4F96ECBCD265CC584C1C3A4D1AC316E92F0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*..qn..."n.."n.."...#l.."g.."e.."n.."B.."<..#c.."<..#~.."<..#q.."<..#o.." <.g"o.."<..#o.."Richn.."..... .....PE..d...Y.-a....." ..... `.....p.....`A.....B..4....J.....p..X....X...#.....h,..T..... .....8.....text..... ..`.rdata...@.....B.....@..@.data...@....`.....@.....@....pdata..X....p.....D..... @..@_RDATA.....P.....@..@.rsrc.....R.....@..@.reloc.....V.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_bz2.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	80784
Entropy (8bit):	6.45456109441925
Encrypted:	false
SSDEEP:	1536:hwz7h8B7BjhJCZePYgl/5S8Gh2Nv0DFlGtVQ7Sygj:hwz18BrJCJglhlGINv0RIGtVQej
MD5:	BCF0D58A4C415072DAE95DB0C5CC7DB3
SHA1:	8CE298B7729C3771391A0DECD82AB4AE8028C057
SHA-256:	D7FAF016EF85FDBB6636F74FC17AFC245530B1676EC56FC2CC756FE41CD7BF5A
SHA-512:	C54D76E50F49249C4E80FC6CE03A5FDEC0A79D2FF0880C2FC57D43227A1388869E8F7C3F133EF8760441964DA0BF3FC23EF8D3C3E72CE1659D40E8912CB3E9C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>E.mE.mE.mL.=mO.m...lG.m#.SmF.m...ll.m...lM.m...lA.m...lF.m ...lG.mE.m..m...lM.m...lD.m..QmD.m...lD.mRichE.m.....PE..d....y.a....." .....^.....P.....S7....`.....@...H.....0..... .. ,.....@.....`...T.....8.....text...U..... ..`.rdata...>.....@.....@..@.data.....@....pdata..,.... ....@..@.rsrc.....0.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_cffi_backend.cp310-win_amd64.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	181248
Entropy (8bit):	6.191174351377468
Encrypted:	false
SSDEEP:	3072:fp5LZ3sgWSqjfy8dBbm/6WnUsHozssS7piSTLkKyS7TlSyQH:fptZ8gW9jrBbQnfIzLliSTLLymlSy
MD5:	6F1B90884343F717C5DC14F94EF5ACEA
SHA1:	CCA1A4DCF7A32BF698E75D58C5F130FB3572E423
SHA-256:	2093E7E4F5359B38F0819BDEF8314FDA332A1427F22E09AFC416E1EDD5910FE1
SHA-512:	E2C673B75162D3432BAB497BAD3F5F15A9571910D25F1DFFB655755C74457AC78E5311BD5B38D29A91AEC4D3EF883AE5C062B9A3255B5800145EB997863A7D7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.....C...C...C..NC...CI..B...C}. C...CI..B...CI..B...CI..B...C...B...C. ..B...C...C..C...B...C..HC...C...B...C.."C...C...B...CRich...C.....PE..d...o.b....." .....@.....0.....`.....g..l...|g..... ...H..... .....M.....M..8.....text...H..... ..`.rdata.....@..@.data....\.....0...v.....@....pdata. .H.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_ctypes.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	119696
Entropy (8bit):	5.97015025328591
Encrypted:	false
SSDEEP:	3072:RW66GKh4hqyIVQoavMSuthSfrS04ep9x31IGQPm5S:Y6QKtkSu3SfrSGFBS
MD5:	41A9708AF86AE3EBC358E182F67B0FB2
SHA1:	ACCAB901E2746F7DA03FAB8301F81A737B6CC180
SHA-256:	0BD4ED11F2FB097F235B62EB26A00C0CB16815BBF90AB29F191AF823A9FED8CF
SHA-512:	835F9AA33FDFBB096C31F8AC9A50DB9FAC35918FC78BCE03DAE55EA917F738A41F01AEE4234A5A91FFA5BDBBD8E529399205592EB0CAE3224552C35C098B78 43
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P...1c..1c..1c..I...1c..Db..1c..Df..1c..Dg..1c..D`..1c.vDb..1c..Cg..1c. .Cb..1c.VXb..1c..1b.$1c.vDn..1c.vDc..1c.vD...1c.vDa..1c.Rich.1c.....PE..d....y.a....." ..... [.....`..... ....Q.....Q.....T..... ..8.....@.....text..... ..`.rdata...k.....l.....@..@.data...T>...p...8...\..... .....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_decimal.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	250768
Entropy (8bit):	6.527857952800466
Encrypted:	false
SSDEEP:	6144:MJFPEV3nLF0eMMCtGzohEgCmUQjYK9qWMa3pLW1AtSrYB4BRWr8k:cPgXLF035tVZCRBQC06nWr8k
MD5:	D976C5F77A6370CF6F28A5714BF49AE3
SHA1:	79273EB123A68BA5CB91FF37EE0A82CEE880C2CC
SHA-256:	FE2BCCB2E204A736ED86A8D16EFFEAFE83B30B44F809349E172142665DE8458A
SHA-512:	57DF90F9FAF31F81F245A39A14C0784A3FACE4F76F00430DE8CFF2E86B55FA3269CD595119FD093E03709DEBF0888618917CAE5EA5E68F43A8E928861CAA01C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t!=.0@S.0@S.0@S.98..>@S.b5R.2@S.b5V.<@S.b5W.8@S.b5P. 4@S..5R.3@S..2R.2@S.0@R..@S..5P.1@S..5^.?@S..5S.1@S..5..1@S..5Q.1@S.Rich0@S.....PE..d....y.a....." .....\|...:.....l.....-.....`... .....T..P....T.....'.....<... ...T.....8.....text....{.....\|..... ..`.rdata.....@..@.dat a....)...p...$...X.....@....pdata...'.....(...|.....@..@.rsrc.....@..@.reloc..<.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_hashlib.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	60304
Entropy (8bit):	6.093275200649072
Encrypted:	false
SSDEEP:	768:JV/wp93dN0yIITgu/w521DxBjWO/Z1bbr1IG5ltYiSyvJhKy:GNdeyIaVww1TjWMr1IG5lt7Syf
MD5:	F63DA7F9A4E64148255E9D3885E7A008
SHA1:	756DC192E7B2932DF147C48F05EC5E38E9AA06E6
SHA-256:	FA0BB4BF93A6739CE5ADE6A7A69272BBC1227D09C7AFC1C027D6CEA41141BCC6
SHA-512:	23D06DEF20C3668613392A02832777B27AD5353E1DC246316043B606890445D195A1066FCA65300A5D429319AA2AE2505F9FA3A5AB0F97ABA2717B64AAA07E8D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....bGq.&&..&&..&&../^.."&..tS..$&..tS..-&..tS...&..tS..%&..S..$&. ..T..$&...Q..%&..&&..&..S..'&..S..'&..S..'&..S..'&..Rich&&.....PE..d....y.a....." .....P...~.....<.....`.....P..... .....T....k..T.....k..8.....`.....text....N.....P..... ..`.rdata...O...`...P...T.....@..@.data...H..... ..@....pdata.....@..@.rsrc.....@..@.reloc..T.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_lzma.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	154000
Entropy (8bit):	6.8078458773005055
Encrypted:	false
SSDEEP:	3072:GD6xBrqs+vs0H0q8bnpbVZbXsAIPznfo9mNoK5vSpxpRIGe1y2:GD63rcRLCV+7wYOK50P2
MD5:	BA3797D77B4B1F3B089A73C39277B343
SHA1:	364A052731CFE40994C6FEF4C51519F7546CD0B1
SHA-256:	F904B02720B6498634FC045E3CC2A21C04505C6BE81626FE99BDB7C12CC26DC6
SHA-512:	5688AE25405AE8C5491898C678402C7A62EC966A8EC77891D9FD397805A5CFCF02D7AE8E2AA27377D65E6CE05B34A7FFDEDF3942A091741AF0D5BCE41628BF D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.....Z.....3.....Z.....Z.....Z.....Z.. ....Rich.....PE..d....y.a....." .....^.....2.....`.....L.....x...`.....@.....:.....p..D...H{..T.....{.. 8.....p.....text....]......^..... ..`.rdata.....p.....b.....@..@.data.....0.....@....pdata.....@.....@..@.rsrc.....`..... .....@..@.reloc..D....p.....8.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_pytransform.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	1165824
Entropy (8bit):	7.056422721818035
Encrypted:	false
SSDEEP:	24576:LsZDXB6wmcZzdcZ7fUoPHUEXLznTrenIGHSQt:QZDXB6wmcUfTCHHt
MD5:	B07455B8C47BBBE0AE685314988C397E
SHA1:	5464EA83A88BC7BD1054A119C8BB38952C3DCB17
SHA-256:	30EFA93EC5E967CA5BBBFEFC9970CEDB0806F89E7F10EC59B708A5F853E0DF32
SHA-512:	42D279952BA8359AD3F71E6696888C662E6F829F614444BE16C97D553C71E06BBA0A2F01BFF6C7FE3CC435C04DF8A4B1FEFFCDDA1E54B4167EE206FAEC59D7 5E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."....b.....0.....p.....[..... .....+.....'.....`..(.....d.....text...ha.....b.....`.P`.data.....f.....@.`..rdata.. p.....h.....@.`@.pdata...'.....(...V.....@.0@.xdata..L,.....~.....@.0@.bss....h.....`..edata..+.....@.0@.idata..... .....@.0..CRT....X.....@.@..tls.....@.@..reloc.....@.0B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_queue.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27536
Entropy (8bit):	6.261734078833693
Encrypted:	false
SSDEEP:	384:smfqkQfdUCUFYS9F6XP6rEhSSVYptTDbPdIG7UcIYiSy1pCQ7Rhp7:spdUC+y6rEhSSVYTPdIG7UNYiSyvdhp7
MD5:	E6BB918CC02CD270BAD449875577427C
SHA1:	5B22420AE4170858A6A2AA04A54ADC26B9A8051C
SHA-256:	2D8B41DAD8A8506870E6F2E2A5856C6C6C68A219F18BD88AD79C63CFA1366B1F
SHA-512:	B19353E0DF213525C466D5CB80F362AB1A22EAF9940F742B59DF1C2842E49594DB87A5119289DCA616FDFA3E808C7CEB26906E0FF8723AFC80AF768496FACA9 C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.a.....@.....@.....@.....@.....Z..... .....Rich.....PE..d....y.a....." .....6.....D!...`.....@C..L....C..d....p.....`.....L.....3..T..... .....p3..8.....0.. .....text...*..... ..`.rdata.....0.....@..@.data.....P.....8.....@....pdata.....`.....<.....@..@.rsrc... .....p.....@.....@..@.reloc.....J.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_socket.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	75152
Entropy (8bit):	6.147254943521508
Encrypted:	false
SSDEEP:	1536:z1XB7kEDATyhAZ9/s+S+pxyXc/+lf7PdIGQwP7Syr:ZXB4EDXhAZ9/sT+px8c/Sz1IGQwP9
MD5:	79C2FF05157EF4BA0A940D1C427C404E
SHA1:	17DA75D598DEAA480CDD43E282398E860763297B
SHA-256:	F3E0E2F3E70AB142E7CE1A4D551C5623A3317FB398D359E3BD8E26D21847F707
SHA-512:	F91FC9C65818E74DDC08BBE1CCEA49F5F60D6979BC27E1CDB2EF40C2C8A957BD3BE7AEA5036394ABAB52D51895290D245FD5C9F84CC3CC554597AE6F85C1 9E1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.....nk.....c.....c.....c.....c.....xc.....t....d.....xc.....xc.. ....xc.....xc.....Rich.....PE..d....y.a....." .....l..... &.....P.....v7....`.....P.....0..... ..<.....@.....T..... .....8.....text...Fj.....l..... ..`.rdata..Ts.....t...p.....@..@.data.....@....pdata..<.... .....@..@.rs rc.....0.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_ssl.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	156560
Entropy (8bit):	5.942876418107184
Encrypted:	false
SSDEEP:	3072:RYNRsSzeOfeC1uHv8MmouyETvb8VqH70NmHh4kwooSLteSdo9dRlGt7+ig:RYjPzeOfeYMvZuyvV0Dtho9dVg
MD5:	1ED0EF72A40268E300A611BA4AB20DFD
SHA1:	4D04D5911A6ED422308EA11D7B15821AF8F62585
SHA-256:	5860FE208122219A4071CC369D5001EDC3B08C13BD96156ABD1375E35401ACD0
SHA-512:	F72EA051ED50A09561414FC41D837C03CE44BE9D8E4C39F59133DD8A092C9F13FC942C58DC8517EDC149CAA3BF7D94FA6BDBE88CABC8CB3C6A02428676572 3E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.D...*...*...*.....*.D.+...*.D./...*.D.....*.D.)...*..+...*...+...*...+..*...+. ..*..'...*..*...*.....*..(...*.Rich..*.....PE..d....y.a....." .....I*.....`.....d.....`.....P.....D.....p..8.....T..... .....8.....x.....text...T..... ..`.rdata.....@..@.data....j.....f.....@....pdata.....P..... .....@..@ .rsrc.....`.....,.....@..@.reloc..8....p.....6.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202_uuid.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	21392
Entropy (8bit):	6.271052728197517
Encrypted:	false
SSDEEP:	384:WvEaNKFDyeTxXK5DFlGewqcIYiSy1pCQIQhwv:WTNK4e9XK5DFlGewgYiSyvJhwv
MD5:	0162EDE31051183D9E23BADA8B7FD0AA
SHA1:	F4AD798660B81E9BFBBEC6E44BD5C4BFFCF5F3B2
SHA-256:	8F1C0151485055E65F174D779CFEFD2FAE601CA52F556EE3880E417EA6E43187
SHA-512:	17A5AF2CD7A9603F31BB3B796DAE13BA157886A4BC05665780FD54C1E30F1FAD76648D56E35C18E2B0C1379D1A83EC98CC97AB2DC4E968FE8D648DB3341C22 01
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z4F.>U(.>U(.>U(.7-..<U(.l).<U(.l -.5U(.l ,.6U(.l +.=U(..).<U(..').;U(.>U)..U(.. .?U(.. (.?U(.. ..?U(.. *.?U(.Rich>U(.....PE..d....y.a....." .....&..... .....p.....` ..... ).L...l)..x....P.....@.....4.....`..<....".T.....`"..8..... ..0.....text...X..... ..`.rdata..f.... .....@..@.data.....0.....$.....@....pdata.....@..... .&.....@..@.rsrc.....P.....(.....@..@.reloc..<....`.....2.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\base_library.zip

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=store
Category:	dropped
Size (bytes):	831571
Entropy (8bit):	5.700814153772732
Encrypted:	false
SSDEEP:	12288:gVghg9FMWyrVqF3IUQA4a2Y4dgVwOlfJEW4XSgMNn:gVghVVrDLa2oVwOlfJEW4fMNn
MD5:	0FFE117C16F44A32C0AED0080D4AE966
SHA1:	7F8317DE4FFA0ED54AA53AF202AED0F297ED1913
SHA-256:	28C1EFDFCF212AFFBD33649E3BAFA33D55F00AF5EC6BBF94692DF56FDC3D3B59
SHA-512:	4FD0C1C4C512DD0A7E35E2206619AFBFC9513BD96B160F9851CECBBA18ED2F128BB3817B30DA925D1515C3D484497C1B9C1139328BA4478023340693D4ECBEC
Malicious:	false
Preview:	PK.....!.Q..M....._collections_abc.pyco.....6.-.....@.....d.Z.d.d.l.m.Z.m.Z...d.d.l.Z.e.e.e.....Z.e.d...Z.d.d...Z.e.e...Z.[.g.d...Z.d.Z.e.e.d.....Z.e.e.e.....Z.e.e.i.....Z.e.e.i.....Z.e.e.i.....Z.e.e.g.....Z.e.e.e.g.....Z.e.e.e.d.....Z.e.e.e.d.d.>.....Z.e.e.e.....Z.e.e.d.....Z e.e.d.....Z!e.e.e"....Z#e.i.....Z$e.i.....Z%e.i.....Z&.e.j'..Z(e.d.d.....Z)d.d...Z*e*..Z*e.e*..Z+e*.,....[*d.d...Z-e-..Z-e.e-..Z.[-d.d...Z/G.d.d...d.e.d...Z0G.d.d...d.e.d...Z1G.d.d...d.e1..Z2e2.3e+....G.d.d...d.e.d...Z4G.d.d ..d e4..Z5G.d!d"..d"e5..Z6e6.3e.....G.d#d$..d$e.d...Z7G.d%d&..d&e7..Z8e8.3e.....e8.3e.....e8.3e.....e8.3e.....e8.3e.....e8.3e.....e8.3e.....e8.3e.....e8.3e ....e8.3e!..e8.3e#....G.d'd(..d(e7..Z9G.d)d*..d*e8..Z:e:.3e)....G.d+d,..d,e.d...Z;G.d-d...d.e.d...Z<G.d/d0..d0e;e7e<..Z=G.d1d2..d2e...Z>d3d4..Z?d5d6..Z@d7d8..ZAG.d9d:..d:e.d...ZBG.d;d<..d<e=..ZCeC.3eD....G.d=d>..d>eC..ZEeE.3e.....G.d?d@..d@e=..ZFeF

C:\Users\user\AppData\Local\Temp_MEI28202\certifi\cacert.pem

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	285222
Entropy (8bit):	6.049584029751259
Encrypted:	false
SSDEEP:	6144:QW1H/M8f9R0mNpliXCRrwADwYCuMEigT/Q5MSRqNb7d8l:QWN/vRLNL4CRrBC5MWavd0
MD5:	B18E918767D99291F8771414B76A8E65
SHA1:	EA544791B23E4A8F47ACE99B9D08B3609D511293
SHA-256:	A59FDE883A0EF9D74AB9DAD009689E00173D28595B57416C98B2EE83280C6E4C
SHA-512:	78A4EAC65754FB8D37C1DA85534D6E1DD0EB2B3535EF59D75C34A91D716AFC94258599B1078C03A4B81E142945B13E671EC46B5F2FCB8C8C46150AE7506E0DD
Malicious:	false
Preview:	.# Issuer: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA.# Subject: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA.# Label: "GlobalSign Root CA".# Serial: 48357032784597076690052O4.# MD5 Fingerprint: 3e:45:52:15:09:51:92:e1:b7:5d:37:9f:b1:87:29:8a.# SHA1 Fingerprint: b1:bc:96:8b:d4:f4:9d:62:2a:a8:9a:81:f2:15:01:52:a4:1d:82:9c.# SHA256 Fingerprint: eb:d4:10:40:e4:bb:3e:c7:42:c9:e3:81:d3:1e:f2:a4:1a:48:b6:68:5c:96:e7:ce:f3:c1:df:6c:d4:33:1c:99.-----BEGIN CERTIFICATE-----.MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG.A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv.b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjgxMjAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i.YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT.aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ.jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp.xy0Sy6scTHAHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\INSTALLER

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:Mn:M
MD5:	365C9BFEB7D89244F2CE01C1DE44CB85
SHA1:	D7A03141D5D6B1E88B6B59EF08B6681DF212C599
SHA-256:	CEEBAE7B8927A3227E5303CF5E0F1F7B34BB542AD7250AC03FBCDE36EC2F1508
SHA-512:	D220D322A4053D84130567D626A9F7BB2FB8F0B854DA1621F001826DC61B0ED6D3F91793627E6F0AC2AC27AEA2B986B6A7A63427F05FE004D8A2ADFBDADC13C1
Malicious:	false
Preview:	pip.

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\LICENSE	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	329
Entropy (8bit):	4.603126991268486
Encrypted:	false
SSDEEP:	6:h9Co8FMjkDYc5tWreLBF/flKY2mHxXaASvUSBT5+FLkYjivW:h9aWjM/mrGz3lKZvUSBT5+Jxi+
MD5:	8F65F43B29FEA29D36A0E6E551CCA681
SHA1:	DEF52585EE54F0B8841A097B871ABD5F5E94DB10
SHA-256:	970C6BC0FAB59117A0B65E9A6D5F787A991BEBE82AFF32A01C4E1A6E02F4E105
SHA-512:	A5DED62228355C40533E53592164CE9BF511D5F0B98478AD91558626DA02BD6D85185B8DA767338692C60ECB4AB6CBFB2E97EEE6530101A3AFF04CE8087687E
Malicious:	false
Preview:	This software is made available under the terms of *either* of the licenses..found in LICENSE.APACHE or LICENSE.BSD. Contributions to cryptography are made..under the terms of *both* these licenses.....The code used in the OS random engine is derived from CPython, and is licensed..under the terms of the PSF License Agreement...

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\LICENSE.APACHE	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	11562
Entropy (8bit):	4.476412280491683
Encrypted:	false
SSDEEP:	192:qf9fG4QSAVOSbwF1wOFXuFJyQtxmG3ep/7rlzKfHbxc+Xq0rhlkT8SgfH2:k1u9b01DY/rGBt+dc+aclkT8Sg+
MD5:	D3DC5ABBDBEF739DCFF4631C8026D71C
SHA1:	DABFE012BF7944B938C95845769414C1D5FA8BB9
SHA-256:	E8DE1A7393457E9C88768B78E6BA790622FBEFB040CE48194C2CB0F1B6D4E9FF
SHA-512:	C8245BD674A2EDB3CE191EC42E701E3E78AEFA3822846604EE0A8FBBB5D62B5372BE07EC8D4D1DD8F6E1DDFE65DAB1136FEE6917FF24445286EFEF99F908E CA2
Malicious:	false
Preview:	.. Apache License.. Version 2.0, January 2004.. https://www.apache.org/licenses/.... TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION.... 1. Definitions..... "License" shall mean the terms and conditions for use, reproduction,.. and distribution as defined by Sections 1 through 9 of this document..... "Licensor" shall mean the copyright owner or entity authorized by.. the copyright owner that is granting the L icense..... "Legal Entity" shall mean the union of the acting entity and all.. other entities that control, are controlled by, or are under common.. control with that entity. For the purposes of this definition,.. "control" means (i) the power, direct or indirect, to cause the.. direction or management of such entity, whether by cont ract or.. otherwise, or (ii) ownership of fifty percent (50%) or more of the.. outstanding shares, o

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\LICENSE.BSD	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1559
Entropy (8bit):	5.097091815591564
Encrypted:	false
SSDEEP:	48:NOWJbPrYJ0NCPiB432sVoY32s3EiP3tQHy:gWJbPrYJUNu3J3zVSS
MD5:	07BFF60D258208652DF09D36F7F94844
SHA1:	E37EC74CF1EC6B540A511EA75E04C3429DB39C57
SHA-256:	661D18932DD84BB263A8EE418AB7774ED94EEC33C83FD1DB5B533F78EB774CA4
SHA-512:	049659D6AC6681E209F30E1A6A12BA6118BEB96F032FD3E2583686EA562068E311C61CCD0785B0FC343ECBA094955C972ABCF9AE9B0A4503C56131F1A59A6F8
Malicious:	false
Preview:	Copyright (c) Individual contributors...All rights reserved.....Redistribution and use in source and binary forms, with or without..modification, are permitted provided that the following conditions are met:.... 1. Redistributions of source code must retain the above copyright notice,.. this list of conditions and the following disclaimer..... 2. Redistributions in binary form must reproduce the above copyright.. notice, this list of conditions and the following disclaimer in the.. documentation and/or other materials provided with the distribution..... 3. Neither the name of PyCA Cryptography nor the names of its contributors.. may be used to endorse or promote produc ts derived from this software.. without specific prior written permission.....THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND..ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED..WARRANTIES OF MERCHANTABILITY AND FI TNESS FOR

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\LICENSE.PSF	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators

Category:	dropped
Size (bytes):	2456
Entropy (8bit):	5.053763055088611
Encrypted:	false
SSDEEP:	48:xUXkp7vXkzpXFlYPXc/XFbwDt3XF2iDPGkvAuXF1f0T2sMtQVHiioTxmynXh2XFQ:KXwDXklHYPXaAt3ZSkYuyCQ4hTcynx26
MD5:	36F8D9BAB4000E435033D3CDB2E85E9B
SHA1:	003076B91D93233F389AB5DB052C04386620BB76
SHA-256:	C2ED0F2724ACA6CEC716CE169FD22C91B79A21FF625C3725D5C71BE1A7977430
SHA-512:	48396B8D7DD14A10C3941788DFED9FF0699C413328FA086CF1D7DCB5E4ED538AEC98541A758B169E271C3DD9BE6056E2EEA0853A6F6DA9C44D865718425DBF E
Malicious:	false
Preview:	1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and.. the Individual or Organization ("Licensee") accessing and otherwise using P ython.. 2.7.12 software in source or binary form and its associated documentation.....2. Subject to the terms and conditions of this License Agreement, PSF hereby.. g rants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,.. analyze, test, perform and/or display publicly, prepare derivative works,.. distribute, and otherwise use Python 2.7.12 alone or in any derivative.. version, provided, however, that PSF's License Agreement and PSF's notice of.. copyright, i.e., "Copyright . 2001-2016 Python Software Foundation; All Rights.. Reserved" are retained in Python 2.7.12 alone or in any derivative version.. prepared by Licensee.....3. In the event Licensee prepares a derivative work that is based on or.. incorporates Python 2.7.12 or any part thereof, and wants to make the.. derivative work

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\METADATA

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	5434
Entropy (8bit):	5.111366191178416
Encrypted:	false
SSDEEP:	96:DDhVUvQIUQIhQIKQILbQIRIaMmPktjxsx5nv1AnivAEYaCjF0ErDmpkIE2jQecwX:oYcPuPfsBvunivAEYaCjF0ErDmpkIE2x
MD5:	103327F82BD07D33530E95181C94F9A5
SHA1:	852A8DCE3B0232BD6E5943CF61FB51778D53EB9B
SHA-256:	C5344000C01BDDC1EA5B57170A174AF535CE586DA0861CFEB1D7E6457BD7AEA5
SHA-512:	986EFCD2816F5A4A765CDA90BBBADD1E4F5D3553E2ECA49F6F277CBC7B33D5DDF38E472FC2CE1F13AFC1ABABC74C04020E0A9B48E0A22F8E2FF14A897B16 7FD3
Malicious:	false
Preview:	Metadata-Version: 2.1.Name: cryptography.Version: 37.0.4.Summary: cryptography is a package which provides cryptographic recipes and primitives to Python develo pers..Home-page: https://github.com/pyca/cryptography.Author: The Python Cryptographic Authority and individual contributors.Author-email: cryptography-dev@pyth on.org.License: BSD-3-Clause OR Apache-2.0.Project-URL: Documentation, https://cryptography.io/.Project-URL: Source, https://github.com/pyca/cryptography/.Project- URL: Issues, https://github.com/pyca/cryptography/issues.Project-URL: Changelog, https://cryptography.io/en/latest/changelog/.Classifier: Development Status :: 5 - Pro duction/Stable.Classifier: Intended Audience :: Developers.Classifier: License :: OSI Approved :: Apache Software License.Classifier: License :: OSI Approved :: BSD License.Classifier: Natural Language :: English.Classifier: Operating System :: MacOS :: MacOS X.Classifier: Operating System :: POSIX.Classifier: Operating System :: POSIX :: BSD.Class

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\RECORD

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	15889
Entropy (8bit):	5.542903319592049
Encrypted:	false
SSDEEP:	384:DXNhudIBxy0jX1sjzarQ4Oy3W1HepPNyZGBDLkae:Dvu6BjTLLC
MD5:	28DD4D29EDE55272C2BDCD4128D20BFF
SHA1:	715A6C1D5D8CD44CBFC4872BBE803AB5716F7B49
SHA-256:	DEF15B76024668207D2EAA70A78E867415E17B6C9651F3D17C49B54F1FC3D2B4
SHA-512:	B4E6216E4D80006A25916C61386D6A728394834A424164E7E067C1770200427FF3BF39810A92A3F69B14701813075661146FEB186949A135CA841B1C004C6E19
Malicious:	false
Preview:	cryptography-37.0.4.dist-info/INSTALLER,sha256=zuuue4knoyJ-UwPPXg8fezS7VCrXJQrAP7zeNuwvFQg,4..cryptography-37.0.4.dist-info/LICENSE,sha256=l wxrwPq1kRegtl6abV94epkb6-gq_zKgHE4abgL04QU,329..cryptography-37.0.4.dist-info/LICENSE.APACHE,sha256=6N4ac5NFfpyIdot45rp5BiL777BAzkgZTCyw8bbU 6f8,11562..cryptography-37.0.4.dist-info/LICENSE.BSD,sha256=Zh0Yky3YS7JjqO5Bird3TtlO7DPIP9HbW1M_eOt3TKQ,1559..cryptography-37.0.4.dist-info/LICENSE.PS F,sha256=wu0PJySsps7HFs4Wn9IskbeaIf9iXDcI1ccb4aeXdDA,2456..cryptography-37.0.4.dist-info/METADATA,sha256=xTRAAMAb3cHqW1cXChdK9TXOWG2ghhz-sdf mRXvXrqU,5434..cryptography-37.0.4.dist-info/RECORD,,..cryptography-37.0.4.dist-info/WHEEL,sha256=nYCSW5p8tLyDU-wbqo3uRlCluAzwxLmyyRK2pVs4-A g,100..cryptography-37.0.4.dist-info/top_level.txt,sha256=zYbdX67v4JFZPfsaNue7ZV4-mgoRqYCAhMsNgt22LqA,22..cryptography/__about__.py,sha256=faxkUiE2bBS zSgtjgJ-beVDEW-CO_1hPe1MuwUZbzc0,432..cryptography/__init__.py,sha256=nhedhGi0RRlu5-T65qB364Q-onagWl0wvDZym5NaL2w,777..cryptography/__pycach

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\WHEEL

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped

Size (bytes):	100
Entropy (8bit):	5.000336540814903
Encrypted:	false
SSDEEP:	3:RtEeX7MWcSlViZHKRRP+tkKc5vKQLn:RtBMwlViojWK/SQLn
MD5:	FD7C45A29F7B2371E832F4D0A8B2DB64
SHA1:	D2227C6F4CD8A948E4A4CA6BF2592E9700383EB1
SHA-256:	9D80925B9A7CB4BC8353EC1BAA8DEE4650A5B80CF0C4B9B2C912B6A55B38F808
SHA-512:	AEF644A24B948DC30C2097D53CD5D412C85958E7846720F4E3693F42924597F6924BD24E1B083B2EC57E7BA08C54DBDCA3C1AE73AC2322CD1A575F06BB4D1D0
Malicious:	false
Preview:	Wheel-Version: 1.0.Generator: bdist_wheel (0.37.1).Root-Is-Purelib: false.Tag: cp36-abi3-win_amd64..

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography-37.0.4.dist-info\top_level.txt

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	22
Entropy (8bit):	3.7887549139935035
Encrypted:	false
SSDEEP:	3:DA1JEOv:DUVv
MD5:	6DB3CE9E78C8F56F58CDF1B221C0884B
SHA1:	D8D1BA8EE6C2A5EED9CB39B170EE08012AB41E11
SHA-256:	CD86DD5FAEEFE091593DFB1A36E7BB655E3E9A0A11A9808084CB0D82DDB62EA0
SHA-512:	6F8AB5DA07A237C2BD6DA073A66125EB0CA754389CB84671D68D0DA4122AD6DDA58336900B1100D235814B16EFB970A2C3FBAF91B82366808DAA81A63EAE31AE
Malicious:	false
Preview:	_openssl.cryptography.

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography\hazmat\bindings_openssl.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3962880
Entropy (8bit):	6.5600156596934625
Encrypted:	false
SSDEEP:	49152:LIU6ioeGtlqTVwASOICDs+JhX3wHqg+dhptXdqCHJYN1QwhIC4Fjz80nciTOzNqm:k+lkEs7JYNgFjz80cDh1YFZdZBT
MD5:	8A2C06F1015C438CB38FFE8B1CDAD831
SHA1:	A3FBED5033E9658043D18AF54543D7938037E08F
SHA-256:	811441D49208C88B7B6B7133A9FD8F2FB969659563D3F2C80584D2F12338E020
SHA-512:	7FD89967A4C8A041D6949AE37C0544E7694ADE9055AB828C25ADD4D0359E170BF6543BAFD2EC4B8116ABEFB176B26229C730F3D085983718E0100AAE659F3CE1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P...(7..P...*...P...*...P...*...P...*...P..._$...P...(...P.. .P..MP...P...P...*...S...*...P...*...P...*[..P...*...P..Rich.P.....PE..d....<.b....." ... .T+..L.....pU+.....<.....`.....9.P...`.9.h.....<... ....:..... <.p...p.7.....0.7.@.....p+.p.....text....S+.....T+..... ..`.rdata.....p+.....X+.....@..@.data.....09.....9..... ..@....pdata.....:.....9.....@..@.rsrc.....<.....;.....@..@.reloc..p.... <.....;.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\cryptography\hazmat\bindings_rust.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1593344
Entropy (8bit):	6.148502058477941
Encrypted:	false
SSDEEP:	24576:j/bXNabjIX1FSCD2Ai8tExl6/RA11zz5Wp3BabkGon9wC3f+um4aFu:PQjIX1FSCD2Ai8tE2aYUz
MD5:	3C96F548076A8A0587517DB899FB09AE
SHA1:	36F252F529DD6DFB0E3A5FD0298EE817DCFED8BD
SHA-256:	8168767337ED93D3341C583F1D8B0CF8956C3CDF3BD6428AF7A3DDBAF206CC08
SHA-512:	3EB7665F7D0D70530F7BED28DD0606FAF97D7A2EA1277D302301EDC278AB0AB79DCAECC1F89591211F2B63478F6984395754029B91A127163CC2271D24ED51D

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.G.8...8...8...@v..8...B...8...B...8...B...8...B...8...@...8..RL...8.. .8...8...8..08...B...8...B...8..Rich.8.....PE..d...}<.b....." ... .*...$.....`.....v..X...Hw.....X..... .p..P...`...T.....(... ...@.....@.....text....).....*..... ..`.rdata...H...@...J.....@..@.data.....x.....@....pdata..X..... .....@..@.reloc..P....p.....<.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\libcrypto-1_1.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3438840
Entropy (8bit):	6.094542623790425
Encrypted:	false
SSDEEP:	49152:DTKuk2HvIU6iwpOjPWBdwQN+5X2uyWsrV4+OGyu1BYGx6KCIrA9NPe0Cs5Z1CPwE:Pg+Hb5Wt+2BoBIcU0CsD1CPwDv3uFfJZ
MD5:	63C756D74C729D6D24DA2B8EF596A391
SHA1:	7610BB1CBF7A7FDB2246BE55D8601AF5F1E28A00
SHA-256:	17D0F4C13C213D261427EE186545B13EF0C67A99FE7AD12CD4D7C9EC83034AC8
SHA-512:	D9CF045BB1B6379DD44F49405CB34ACF8570AED88B684D0AB83AF571D43A0D8DF46D43460D3229098BD767DD6E0EF1D8D48BC90B9040A43B5469CEF71774162
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.....3.....^....^.....^....^.\...^....Rich..... .....PE..d....A.a....." .....$.....5.....4...`.....h/..h...:4.@....p4.|....`2.h....\4.....4..O...,.8.....p.,.8..... .....04.....text.....$.....$..... ..`.rdata.....$.....$.....@..@.data...!z....1.,....1.....@....pdata..8....`2.....1.....@..@.idata..^#...04..$.... 3.....@..@.00cfg..c....`4.....3.....@..@.rsrc...|....p4.....3.....@..@.reloc...x....4..z....3.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\libffi-7.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32792
Entropy (8bit):	6.3566777719925565
Encrypted:	false
SSDEEP:	384:2nypDwZH1XYEMXvdQOsNFYzsQDELCvURDa7qscTHstU0NsICwHLZxXYIoBneEAR8:2l0Vn5Q28J8qsqMttktDxOpWDG4yKRF
MD5:	EEF7981412BE8EA459064D3090F4B3AA
SHA1:	C60DA4830CE27AFC234B3C3014C583F7F0A5A925
SHA-256:	F60DD9F2FCBD495674DFC1555EFFB710EB081FC7D4CAE5FA58C438AB50405081
SHA-512:	DC9FF4202F74A13CA9949A123DFF4C0223DA969F49E9348FEAF93DA4470F7BE82CFA1D392566EAAA836D77DDE7193FED15A8395509F72A0E9F97C66C0A096016
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6.3.r}]Ar}]Ar}]A{..Ap}]A .\@p}]A..\@q}]Ar}\AU}]A .X@~}]A .Y@z}]A .^@q}]A..Y@t}]A..^@s}]A..]@s}]A.._@s}]ARichr}]A.....PE..d.....]....." .....F...$.....I.....`.....j.....m..P..... .....f.....b.....b.....`. .....text....D.....F..... ..`.rdata..H...`.....J.....@..@.data.....^.....@....pdata..... .....`.....@..@.reloc.....d.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\libssl-1_1.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	698104
Entropy (8bit):	5.531132600342763
Encrypted:	false
SSDEEP:	12288:tgH+zxL52Y1Ag5EbSJyin89m8GXfbmednWAeO6GKaf525eWP8U2lvzI:DD1Ag5h/L5mO6GVf52se8U2lvzI
MD5:	86556DA811797C5E168135360ACAC6F2
SHA1:	42D868FC25C490DB60030EF77FBA768374E7FE03
SHA-256:	A594FC6FA4851B3095279F6DC668272EE975E7E03B850DA4945F49578ABE48CB
SHA-512:	4BA4D6BFFF563A3F9C139393DA05321DB160F5AE8340E17B82F46BCAF30CBCC828B2FC4A4F86080E4826F0048355118EF21A533DEF5E4C9D2496B98951344690
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!9._@W^_@W^_@W^V8.^S@W^.7V_]@W^.2V_]@W^.7 R_T@W^.7S_W@W^.7T_[@W^.7V_\@W^_@V^.AW^.7S_s@W^.7W_^@W^.7.^^@W^.7U_^@W^Rich_@W^.....PE..d....A.a....." .....<...T.....<..... .....)&....`.....00...N..HE.....s.....|M.....t...t...8.....8.....0..H.....text...:.....<..... ..`.rdata..:. ...P...0...@.....@..@.data...AM.....D...p.....@....pdata..dV.....X.....@..@.idata..PW...0...X.....@..@.00cfg..c.....d.....@..@.rsrc...s. .....f.....@..@.reloc..]....n.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\pyexpat.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	192400
Entropy (8bit):	6.331661708582381
Encrypted:	false
SSDEEP:	3072:7UV1H8t//ZpdhxqMO2lr9JuB9OSH4ZCXRfWiTayyTvfvaycv0XOgeEnnRPcsR+2U:yVG/Ddh5r9JuB0SDfV9yTvfvx+Zj
MD5:	F3630FA0CA9CB85BFC865D00EF71F0AA
SHA1:	F176FDB823417ABEB54DAED210CF0BA3B6E02769
SHA-256:	AC1DFB6CDEEADBC386DBD1AFDDA4D25BA5B9B43A47C97302830D95E2A7F2D056
SHA-512:	B8472A69000108D462940F4D2B5A611E00D630DF1F8D6041BE4F7B05A9FD9F8E8AA5DE5FE880323569AC1B6857A09B7B9D27B3268D2A83A81007D94A8B8DA0F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B.J.B.J.B.J.::J.B.J.7.K.B.J.7.K.B.J.7.K.B.J.7.K.B.J57.K.B .J\0.K.B.J.B.J.B.J57.K.B.J57.K.B.J57VJ.B.J57.K.B.JRich.B.J.....PE..d....y.a....." .....p.....8....`.....P...P. .....4..T.....P5..8..... .....text..... ..`.rdata..|.... .....@..@.data.....@....p data.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp_MEI28202\python3.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	62352
Entropy (8bit):	5.969350602670095
Encrypted:	false
SSDEEP:	768:4st8LeBLeeFtp5V1BfO2yvSk70QZF1nEyjnskQkr/RFB1qucwdBeCw0myou6ZwJ1:Ttwewnvtjnsfw9PdIGQ0P7Sy1R
MD5:	C38E9571F33898EB9F3DA53DC29B512F
SHA1:	5BE348C829B6DFA008D0DD239414AD388E5D7ACE
SHA-256:	70596AEA8C5CA8F3BF88E46A0606522413B50208EC9FCC6B706F7A064CF83B79
SHA-512:	1704BE273E3485013282C269FC974558683204639FCCFB46E6EB640C64A0769A21572A07EE62FE1D5EB1EED4D1419F2293D6E4FD8193CAAFE128C6D66BD48F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d...d...d.K.I...d.K.d...d.K.....d.K.f...d.Rich..d.....PE..d....y.a..... ...." .....`.....`...`.....T.....rdata..... .....@..@.rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp_MEI28202\python310.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4453776
Entropy (8bit):	6.4554098557218
Encrypted:	false
SSDEEP:	49152:wplyWz2QcN6iPdzYjz0AMs9Kt2KnX0OCpFLoFnAcECdNCsugztL0DD9fIysVHkDx:sximj29G5H+ywH+MWqlgdMW
MD5:	C6C37B848273E2509A7B25ABE8BF2410
SHA1:	B27CFBD31336DA1E9B1F90E8F649A27154411D03
SHA-256:	B7A7F3707BEAB109B66DE3E340E3022DD83C3A18F444FEB9E982C29CF23C29B8
SHA-512:	222AD791304963A4B8C1C6055E02C0C4C47FCE2BB404BD4F89C022FF9706E29CA6FA36C72350FBF296C8A0E3E48E3756F969C003DD1EB056CD026EFE0B7EBA 40
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U...4...4...4...A...4...[n..4...A...4...A...4...A...4...L...4..zF...4...4...5...A ..i4...A...4...Al..4...A...4..Rich.4.....PE..d....y.a....." ....j#..^!....I.....E.....ND...`.....<.....X.=.\|....pD.....PB.....C..... ..D..t....$.T.....0.$.8.....#.(.....text...>h#.....j#..... ..`.rdata...+....#...,...n#.....@..@.data.....=.....=.....@....pdata..... .PB.....DA.....@..@PyRuntim`....`D.....RC.....@....rsrc.....pD.....VC.....@..@.reloc...t....D..v...`C.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\pywintypes310.dll

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	137216
Entropy (8bit):	6.005880156088182
Encrypted:	false
SSDEEP:	3072:bnfstBwsNJzuMZnYrrC0DdZLN+yeLEKoPUZlB+u:zGys7KoYrrC0LxeYK4UZlB
MD5:	A44F3026BAF0B288D7538C7277DDAF41
SHA1:	C23FBDD6A1B0DC69753A00108DCE99D7EC7F5EE3
SHA-256:	2984DF073A029ACF46BCAED4AA868C509C5129555ED70CAC0FE2235ABDBA6E6D
SHA-512:	9699A2629F9F8C74A7D078AE10C9FFE5F30B29C4A2C92D3FCD2096DC2EDCEB71C59FD84E9448BB0C2FB970E2F4ADE8B3C233EBF673C47D83AE40D12A2317C A98
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x...<.z.<.z.<.z.5..0.z.n.{.>.z.,..=.z.n...(.z.n.~.4.z.n.y.>.z.Y.~.=.z... {.>.z.Y.{.7.z.<.{..z...s.1.z...z.=.z...x.=.z.Rich<.z.....PE..d...&Dgc....." ....."....).....`.....`.....dB..D.....@..l.... .....P.. ...Pn..T.....n.....x.....text...\..... ..`.rdata.....@..@.data....-.....(.....@....pdata..... .. ..@..@.rsrc...l....@.....@..@.reloc.. ....P.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\select.pyd

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	26000
Entropy (8bit):	6.339693503329678
Encrypted:	false
SSDEEP:	384:NUTqPjk/7e12hwheCPHqqYBsVRXPdIG7GxIYiSy1pCQFC67hEQ:iTgUC2hwh7HqbYVPdIG7GmYiSyvD7hF
MD5:	431464C4813ED60FBF15A8BF77B0E0CE
SHA1:	9825F6A8898E38C7A7DDC6F0D4B017449FB54794
SHA-256:	1F56DF23A36132F1E5BE4484582C73081516BEE67C25EF79BEEE01180C04C7F0
SHA-512:	53175384699A7BB3B93467065992753B73D8F3A09E95E301A1A0386C6A1224FA9ED8FA42C99C1FFBCFA6377B6129E3DB96E23750E7F23B4130AF77D14AC504A0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ...N...N...N.....N...O...N...K...N...J...N...M...N.t.O...N...O...N.. .O...N.t.C...N.t.N...N.t.....N.t.L...N.Rich..N.....PE..d....y.a....." .....0.....`.....`@..L....@..x....p.....`..... ..F.....H....2..T.....2..8.....0.....text..... ..`.rdata.....0.....@..@.data.....P.....4.....@....pdata..... `.....6.....@..@.rsrc.....p.....:.....@..@.reloc..H.....D.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\selenium\webdriver\common\mutation-listener.js

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1944
Entropy (8bit):	4.675116854336413
Encrypted:	false
SSDEEP:	48:G+SxKWxZZCg10kH11G4UQzNgxgWLlAziLhVGYTo:G+SQWbZC8hHnG4JRgxgWOJ
MD5:	81F59E36BDE07E051C3CB92A4986B327
SHA1:	676E0A28A5A1353E89469ACAAD1B08ADC62C795D
SHA-256:	2C2083C9A49F65C510D68D3620A57D4DFEDC8DC0FCC32524C1CCB11C6329EA07
SHA-512:	02562FC9AC369BC1994934B371DB8D550638430CBC7F7729DD7B3A95E90F4E53A205A62318803D021041DE362B0ED47752AD910CBDC742BEF6645A20AA96A1F
Malicious:	false

Preview:	// Licensed to the Software Freedom Conservancy (SFC) under one.// or more contributor license agreements. See the NOTICE file.// distributed with this work for additional information.// regarding copyright ownership. The SFC licenses this file.// to you under the Apache License, Version 2.0 (the.// "License"); you may not use this file except in compliance.// with the License. You may obtain a copy of the License at.//.// http://www.apache.org/licenses/LICENSE-2.0.//.// Unless required by applicable law or agreed to in writing,.// software distributed under the License is distributed on an.// "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY .// KIND, either express or implied. See the License for the.// specific language governing permissions and limitations.// under the License...(function () {. const observer = new MutationObserver((mutations) => {. for (const mutation of mutations) {. switch (mutation.type) {. case 'attributes':. // Don't report

C:\Users\user\AppData\Local\Temp_MEI28202\selenium\webdriver\firefox\webdriver_prefs.json

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	2826
Entropy (8bit):	4.690644304617203
Encrypted:	false
SSDEEP:	48:9SVI+Lhz3Oa0KUP8OZsUR4lckTgo6OxRLi//FPa+tLkglKgfgfOHSllrK/rTDzL+:/+trOa0KUP8OZ4ZUFPa+tAFEkOy7aTD+
MD5:	648D3DABABB0C714EE9A2D4A8FA4E39F
SHA1:	762AC0A8D883C8C05059F1815A35F6B55464B7C2
SHA-256:	946ADD298A5E2346E3D53D1CBE8AD7C33E4994130511F6D8B79268BE50B7A34C
SHA-512:	51B2ED36C8BB61EBA99406492B2F6928DB0DB413A8F60E30FDAB74D689247B8C83F0E790D8F6AEE370E0F2E27FD565F4A87608CDC547C752514F1476E6DC89A
Malicious:	false
Preview:	{. "frozen": {. "app.update.auto": false,. "app.update.enabled": false,. "browser.displayedE10SNotice": 4,. "browser.download.manager.showWhenStarting": false,. "browser.EULA.override": true,. "browser.EULA.3.accepted": true,. "browser.link.open_external": 2,. "browser.link.open_newwindow": 2,. "browser.offline": false,. "browser.reader.detectedFirstArticle": true,. "browser.safebrowsing.enabled": false,. "browser.safebrowsing.malware.enabled": false,. "browser.search.update": false,. "browser.selfsupport.url" : "",. "browser.sessionstore.resume_from_crash": false,. "browser.shell.checkDefaultBrowser": false,. "browser.tabs.warnOn Close": false,. "browser.tabs.warnOnOpen": false,. "datareporting.healthreport.service.enabled": false,. "datareporting.healthreport.uploadEnabled": false,. " datareporting.healthreport.service.firstRun": false,. "datareporting.healthreport.logging.consoleEnabled": false,. "datareporting.poli

C:\Users\user\AppData\Local\Temp_MEI28202\selenium\webdriver\remote\findElements.js

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with very long lines (2269)
Category:	dropped
Size (bytes):	53824
Entropy (8bit):	5.477971537716615
Encrypted:	false
SSDEEP:	1536:AXJFPWr+DEqXMn9XM3UkGdEMT8TZZ/6B0clWuF2ZCtYuSn6B:ITU7dW62clW02s3
MD5:	9E69F9A88022723BC82E0591C5E157C4
SHA1:	C081C09A148FE317F740A3F0054DF6579BF60A96
SHA-256:	79C706A9230B156A30EE530803CFD87C0AC06BA5FECFED2243D1D60529C1113A
SHA-512:	2856971F9CB3BCA8887F9BB84E66610750366402B4B80892AC1269EB9D6078FD546AECFFB048CE0E5EA9027B276C51414594CC7052292076D74972414FD3C638
Malicious:	false
Preview:	function(){return (function(){var aa=this||self;function ba(a){return"string"==typeof a}function ca(a,b){a=a.split(".");var c=aa;a[0]in c||"undefined"==typeof c.execScrip t||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c[d]&&c[d]!==Object.prototype[d]?c=c[d]:c=c[d]={}:c[d]=b}.function da(a){var b=typeof a;if("object"==b)if(a){if(a instanceof Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object Window]"==c)return"object";if("[obje ct Array]"==c||"number"==typeof a.length&&"undefined"!=typeof a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"arr ay";if("[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"null"; .else if("function"==b&&"undefined"==typeof a.call)return"object";return b}function ea(a){return"function"==da(a)}function ha(a){var b=typeof a;return

C:\Users\user\AppData\Local\Temp_MEI28202\selenium\webdriver\remote\getAttribute.js

Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with very long lines (1587)
Category:	dropped
Size (bytes):	43157
Entropy (8bit):	5.4711439829805295
Encrypted:	false
SSDEEP:	768:V7p/8YXWW4BJinqX46z3wlU0koCF2TPO2bRmeJbNV9c:V7p/JWFBJinqXNm3nCwPgAc
MD5:	F05A5E91E83CD5CA39FBDED566E30E4C
SHA1:	A7273098A868272944881E6F87838E69CDF9DB44
SHA-256:	2186EA70072C63DDB4AD89F2315A7909A9B4A97F52A69957C74DA72641CDAE6A
SHA-512:	72819C5DDA934955C9F35ECD8724AF965634C1C50B530A81D48A4F167CC815A896180E414790BC0E33C8BC4176C8C777AAB01D3C47C7FFE2818C242EDE8160A
Malicious:	false

Preview:	function(){return (function(){var h=this||self;function aa(a){return"string"==typeof a}function ba(a,b){a=a.split(".");var c=h;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c[d]&&c[d]!==Object.prototype[d]?c=c[d]:c=c[d]={}:c[d]=b}.function ca(a){var b=typeof a;if("object"==b)if(a){if(a instanceof Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object Window]"==c)return"object";if("[object Array]"==c||"number"==typeof a.length&&"undefined"!=typeof a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"array";if("[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"null";.else if("function"==b&&"undefined"==typeof a.call)return"object";return b}function da(a){var b=typeof a;return"object"==b&&null!=a||"function"==b}funct

C:\Users\user\AppData\Local\Temp_MEI28202\selenium\webdriver\remote\isDisplayed.js	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	ASCII text, with very long lines (1724)
Category:	dropped
Size (bytes):	43996
Entropy (8bit):	5.482916356843218
Encrypted:	false
SSDEEP:	768:i5WDMeWWcwpdin/XLwXEWb1sHddFZ/R0o7BnF6LRkVZhYiJEKLuP:i50VWWppdin/Xk7buHdp/R0cF6+VZhzW
MD5:	B3122D6B9700A669111247D95460AC05
SHA1:	A14AF0130FC408719B1BA1AF81C03F54AC9D3F20
SHA-256:	EBDA4033FAA32130BFCA4B7A0B3DF41565A99301DF9331054B18F7932B34C388
SHA-512:	B74BACEBDE59767E18151F5A6E9E735C0243ADA4915BC1B9BBBFE276ADF4830D4B071C1A7AFE52E7A7558A8F9D3C464F329748CAB67864BAEBF05D5E398C7ED4
Malicious:	false
Preview:	function(){return (function(){var k=this||self;function aa(a){return"string"==typeof a}function ba(a,b){a=a.split(".");var c=k;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c[d]&&c[d]!==Object.prototype[d]?c=c[d]:c=c[d]={}:c[d]=b}.function ca(a){var b=typeof a;if("object"==b)if(a){if(a instanceof Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object Window]"==c)return"object";if("[object Array]"==c||"number"==typeof a.length&&"undefined"!=typeof a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"array";if("[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"null";.else if("function"==b&&"undefined"==typeof a.call)return"object";return b}function da(a,b,c){return a.call.apply(a.bind,arguments)}function ea(a,b,c){i

C:\Users\user\AppData\Local\Temp_MEI28202\unicodedata.pyd	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1118608
Entropy (8bit):	5.375765997910847
Encrypted:	false
SSDEEP:	12288:ArlBMmuZ63NNQCb5Pfhnzr0ql8L8kdM7IRG5eeme6VZyrIBHdQLhfFE+uOVg:mlBuqZV0m81MMREtV6Vo4uYOVg
MD5:	D1182BA27939104010B6313C466D49FF
SHA1:	7870134F41BA5333294C927DBD77D3F740AC87E7
SHA-256:	1AC171F51CC87F268617B4A635B2331D5991D987D32BB206DD4E38033449C052
SHA-512:	EF26A2C8B0094792E10CEABBF4D11724A9368D96F888240581A15D7A551754C1484F6B2ED1B963A73B686495C7952D9CB940021028D4F230B0B47D0794607D0F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|.$z8OJ)8OJ)8OJ)17.)>OJ)j:K(:OJ)j:O(4OJ)j:N(0OJ)j:I(;OJ).:K(;OJ).=K(:OJ)8OK)iOJ).:G(9OJ).:J(9OJ).:.)9OJ).:H(9OJ)Rich8OJ).....PE..d....y.a....." .....B.....`*.....@.....5.....`.....X...(..... .....0.....0L..T.....L..8.....`..x.....text....A.....B..... ..`.rdata.....`.....F.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp_MEI28202\win32clipboard.pyd	
Process:	C:\Users\user\Desktop\KuponcuBaba.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27648
Entropy (8bit):	5.45361083133999
Encrypted:	false
SSDEEP:	384:A2hm1rbrcX2HtDD7qxukRVCsdRHSAHjB9SJcE4H0Kuyw:+1rbdleFRVCmRD3RGy
MD5:	C8C57F29DA0D5D46ECEB2FD58BA83865
SHA1:	217DFF02763F01A5F91615C27BA912453775A5DE
SHA-256:	E48C71D64001EA62C232EE43FEF7C27BA6268E217B2B81666705BE33D9E12EC9
SHA-512:	EECC4C57609E914B1C9E9E64C30B2257C9AD763C75E919AB50122D72D911723111A86638E3D288F61994EA7FAEAFA2CFDE1CF3D2407D622CB14F901FFF6C454
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.[.&j5.&j5.&j5./..."j5.t.4.$j5.t.0.-j5.t.1..j5.t.6.$j5..4.$j5..4.$j5.C. 4./j5.&j4.Lj5..<.'j5..5.'j5..7.'j5.Rich&j5.....PE..d...B.ec....." .....:.....X.....`.....@Y..\....Y.....t.....x ....M..T.....M.....@.....text....-..... ..`.rdata...(...@..*...2.....@..@.data...H....p.....\.....@....pdata.....`..... .....@..@.rsrc...t.....f.....@..@.reloc..x.....j.....@..B.....

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	7.9935693044459875
TrID:	• Win64 Executable Console (202006/5) 77.37% • InstallShield setup (43055/19) 16.49% • Win64 Executable (generic) (12005/4) 4.60% • Generic Win/DOS Executable (2004/3) 0.77% • DOS Executable Generic (2002/1) 0.77%
File name:	KuponcuBaba.exe
File size:	9945512
MD5:	d6c3bf64cc7cb131d467246ce5a4c455
SHA1:	2ea0b0bda586aeaef818445f48eae6edca8b9901
SHA256:	d91890315262e8a77c565b54baa5f82cbd32451bbe4293bcd8b1918a3d2e0aa1
SHA512:	7048d585c96d7a0c96154e5dd29d47379713f31e68404f04b582d5798c5bfe2980ea8220e78de7962b0b4e2fe8dbf2884298d9f8c25b258a05574da7b310ea7e
SSDEEP:	196608:F4FR1/wbITLwOjUqamvdsCncq4njQthsiHz5n7kMJgyZetlaFPhavejj:iR1obl/hvaCncvnKhsAn7LJ0tMXIej
TLSH:	ACA63344B7A048F8F877517C8027CA1ADAB2B8922722C15B077A83775F433E25E7B759
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@I..@I..@Ir.CH..@Ir.EH..@Ir.DH..@I...I..@I..EH..@I..DH..@I..CH..@Ir.AH..@I..AI..@I..DH..@I..BH..@IRich..@I.....

File Icon

Icon Hash:	f0c6a08292d6c6d4

Static PE Info

General

Entrypoint:	0x14000a330
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x63A3C1AB [Thu Dec 22 02:32:11 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	0bbecc8e9f9f17b0ea9cc3899b15e5cf

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F91D8E4326Ch
dec eax

Instruction
add esp, 28h
jmp 00007F91D8E42BCFh
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
xor ecx, ecx
call dword ptr [0001FDC3h]
dec eax
mov ecx, ebx
call dword ptr [0001FDB2h]
call dword ptr [0001FD3Ch]
dec eax
mov ecx, eax
mov edx, C0000409h
dec eax
add esp, 20h
pop ebx
dec eax
jmp dword ptr [0001FDA8h]
int3
int3
int3
int3
int3
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 38h
mov ecx, 00000017h
call dword ptr [0001FD94h]
test eax, eax
je 00007F91D8E42D69h
mov ecx, 00000002h
int 29h
dec eax
lea ecx, dword ptr [00041CEAh]
call 00007F91D8E42F2Eh
dec eax
mov eax, dword ptr [esp+38h]
dec eax
mov dword ptr [00041DD1h], eax
dec eax
lea eax, dword ptr [esp+38h]
dec eax
add eax, 08h
dec eax
mov dword ptr [00041D61h], eax
dec eax
mov eax, dword ptr [00041DBAh]
dec eax
mov dword ptr [00041C2Bh], eax

Instruction
dec eax
mov eax, dword ptr [esp+40h]
dec eax
mov dword ptr [00041D2Fh], eax
mov dword ptr [00041C05h], C0000409h
mov dword ptr [00041BFFh], 00000001h
mov dword ptr [00000009h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3b8e4	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x1cb8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x4e000	0x20c4	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x54000	0x754	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x392c0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x39180	0x140	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2a000	0x350	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x287b0	0x28800	False	0.5567551601080247	zlib compressed data	6.497436024881472	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2a000	0x1246a	0x12600	False	0.5137117346938775	data	5.832751054611758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x103e8	0xe00	False	0.130859375	data	1.806338290884056	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x4e000	0x20c4	0x2200	False	0.4762178308823529	data	5.314207607074194	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0x51000	0x15c	0x200	False	0.39453125	data	2.8411284312485376	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x1cb8	0x1e00	False	0.334375	data	5.206372071267865	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x54000	0x754	0x800	False	0.54345703125	data	5.23056010770353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

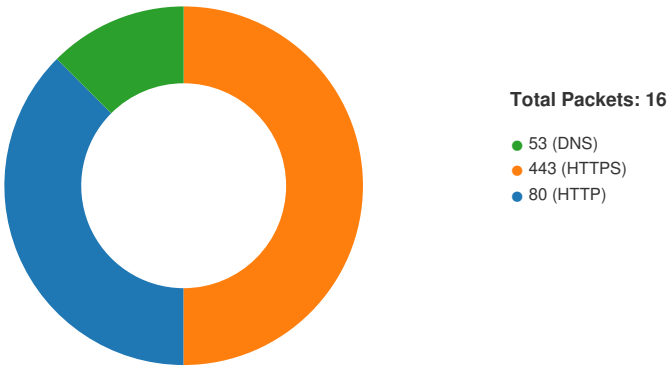
Name	RVA	Size	Type	Language	Country
RT_ICON	0x520e8	0x1628	Device independent bitmap graphic, 64 x 128 x 8, image size 4608		
RT_GROUP_ICON	0x53710	0x14	data		
RT_MANIFEST	0x53724	0x591	XML 1.0 document, ASCII text, with CRLF line terminators		

Imports

DLL	Import
KERNEL32.dll	GetCommandLineW, GetEnvironmentVariableW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, CreateDirectoryW, GetTempPathW, WaitForSingleObject, Sleep, GetExitCodeProcess, CreateProcessW, FreeLibrary, LoadLibraryExW, FindClose, FindFirstFileExW, CloseHandle, GetCurrentProcess, LocalFree, FormatMessageW, MultiByteToWideChar, WideCharToMultiByte, SetEndOfFile, GetProcAddress, GetModuleFileNameW, SetDllDirectoryW, GetStartupInfoW, GetLastError, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetModuleHandleW, RtlUnwindEx, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, EncodePointer, RaiseException, RtlPcToFileHeader, GetCommandLineA, CreateFileW, GetDriveTypeW, GetFileInformationByHandle, GetFileType, PeekNamedPipe, SystemTimeToTzSpecificLocalTime, FileTimeToSystemTime, GetFullPathNameW, RemoveDirectoryW, FindNextFileW, SetStdHandle, SetConsoleCtrlHandler, DeleteFileW, ReadFile, GetStdHandle, WriteFile, ExitProcess, GetModuleHandleExW, HeapFree, GetConsoleMode, ReadConsoleW, SetFilePointerEx, GetConsoleOutputCP, GetFileSizeEx, HeapAlloc, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, CompareStringW, LCMapStringW, GetCurrentDirectoryW, FlushFileBuffers, HeapReAlloc, GetFileAttributesExW, GetStringTypeW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, GetTimeZoneInformation, HeapSize, WriteConsoleW
ADVAPI32.dll	ConvertSidToStringSidW, GetTokenInformation, OpenProcessToken, ConvertStringSecurityDescriptorToSecurityDescriptorW

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:55:27.388087988 CET	49703	80	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.447922945 CET	80	49703	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.448067904 CET	49703	80	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.453983068 CET	49703	80	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.513797045 CET	80	49703	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.513875961 CET	80	49703	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.547445059 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.547523022 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.547619104 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.570631981 CET	49703	80	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.602269888 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.602312088 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.744771957 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.746862888 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.746901989 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.748678923 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.748784065 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.750565052 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.750575066 CET	443	49704	159.253.33.92	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:55:27.750881910 CET	443	49704	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.750904083 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.750943899 CET	49704	443	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.751301050 CET	49703	80	192.168.2.5	159.253.33.92
Jan 5, 2023 08:55:27.810822964 CET	80	49703	159.253.33.92	192.168.2.5
Jan 5, 2023 08:55:27.810923100 CET	49703	80	192.168.2.5	159.253.33.92

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 08:55:27.285583019 CET	51441	53	192.168.2.5	8.8.8.8
Jan 5, 2023 08:55:27.376822948 CET	53	51441	8.8.8.8	192.168.2.5
Jan 5, 2023 08:55:27.527105093 CET	49177	53	192.168.2.5	8.8.8.8
Jan 5, 2023 08:55:27.544616938 CET	53	49177	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 08:55:27.285583019 CET	192.168.2.5	8.8.8.8	0xff23	Standard query (0)	sunucu.troyagame.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:55:27.527105093 CET	192.168.2.5	8.8.8.8	0xdf93	Standard query (0)	sunucu.troyagame.com	A (IP address)	IN (0x0001)	false

DNS Answers

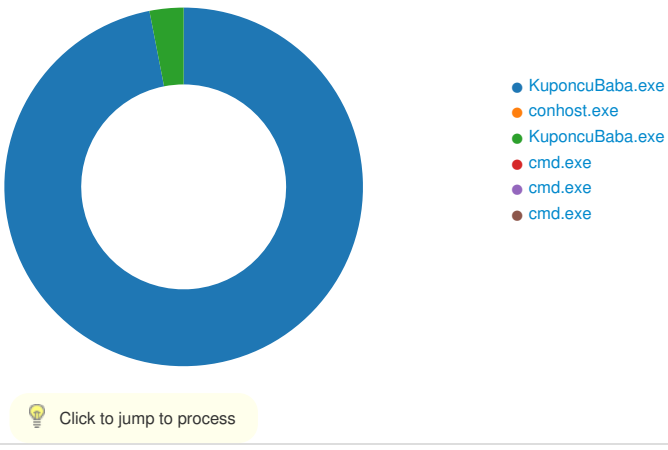
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 08:55:27.376822948 CET	8.8.8.8	192.168.2.5	0xff23	No error (0)	sunucu.troyagame.com		159.253.33.92	A (IP address)	IN (0x0001)	false
Jan 5, 2023 08:55:27.544616938 CET	8.8.8.8	192.168.2.5	0xdf93	No error (0)	sunucu.troyagame.com		159.253.33.92	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- sunucu.troyagame.com

Statistics

Behavior



System Behavior

Analysis Process: KuponcuBaba.exe PID: 2820, Parent PID: 3324

General

Target ID:	1
Start time:	08:55:02
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\KuponcuBaba.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\KuponcuBaba.exe
Imagebase:	0x7ff6f8450000
File size:	9945512 bytes
MD5 hash:	D6C3BF64CC7CB131D467246CE5A4C455
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: conhost.exe PID: 64, Parent PID: 2820

General

Target ID:	3
Start time:	08:55:02
Start date:	05/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: KuponcuBaba.exe PID: 5192, Parent PID: 2820

General

Target ID:	7
Start time:	08:55:08
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\KuponcuBaba.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\KuponcuBaba.exe
Imagebase:	0x7ff6f8450000
File size:	9945512 bytes
MD5 hash:	D6C3BF64CC7CB131D467246CE5A4C455
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	8192	success or wait	1	7FF6F846B6C7	ReadFile
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	4096	success or wait	1	7FF6F846B6C7	ReadFile
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	4096	success or wait	5	7FF6F846B6C7	ReadFile
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	4096	success or wait	2	7FF6F846B6C7	ReadFile
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	4096	success or wait	5	7FF6F846B6C7	ReadFile
C:\Users\user\Desktop\KuponcuBaba.exe	unknown	4096	success or wait	1	7FF6F846B6C7	ReadFile

Analysis Process: cmd.exe PID: **2772**, Parent PID: **5192**

General

Target ID:	8
Start time:	08:55:09
Start date:	05/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c "ver"
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5416**, Parent PID: **5192**

General

Target ID:	9
Start time:	08:55:25
Start date:	05/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c @echo off
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5540**, Parent PID: **5192**

General	
Target ID:	10
Start time:	08:55:26
Start date:	05/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c cls
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly