ID: 829392
Sample Name: Rechung-R1663322504.exe
Cookbook: default.jbs
Time: 05:35:01
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

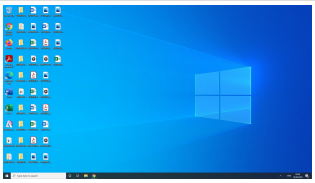
Windows Analysis Report

Rechung-R1663322504.exe

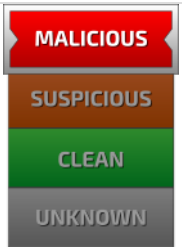
Overview

General Information

Sample Name:	Rechung-R1663322504.exe
Analysis ID:	829392
MD5:	11b5b208de7a…
SHA1:	c578bc317e66…
SHA256:	0a80ba418f561..
Infos:	



Detection



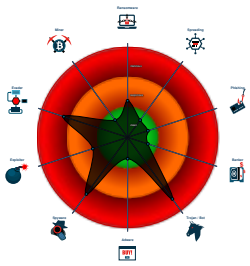
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected BrowserPasswordDum…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- May check the online IP address of…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- Rechung-R1663322504.exe (PID: 6340 cmdline: C:\Users\user\Desktop\Rechung-R1663322504.exe MD5: 11B5B208DE7A85B46104A0597C5DA7DC)
  - CasPol.exe (PID: 6560 cmdline: C:\Users\user\Desktop\Rechung-R1663322504.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 3312 cmdline: C:\Users\user\Desktop\Rechung-R1663322504.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 5220 cmdline: C:\Users\user\Desktop\Rechung-R1663322504.exe MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 5764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - dw20.exe (PID: 9028 cmdline: dw20.exe -x -s 2584 MD5: 89106D4D0BA99F770EAFE946EA81BB65)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.52561610808.0000000037520000.00000004.08000000.00040000.00000000.sdmp	HKTL_NET_GUID_BrowserPass	Detects c# red/black-team tools via typelibguid	Arnim Rupp (https://github.com/ruppde)	• 0x35a3:$typelibguid0: 3cb59871-0dce-453b-857a-2d1e515b0b66
00000007.00000002.52561610808.0000000037520000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	
00000007.00000002.52540526737.0000000034E8C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	
00000007.00000002.52560446262.0000000036F71000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	
00000007.00000002.52540526737.0000000034E46000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.CasPol.exe.37520000.3.unpack	HKTL_NET_GUID_BrowserPass	Detects c# red/black-team tools via typelibguid	Arnim Rupp (https://github.com/ruppde)	• 0x17a3:$typelibguid0: 3cb59871-0dce-453b-857a-2d1e515b0b66
7.2.CasPol.exe.37520000.3.unpack	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	
7.2.CasPol.exe.37520000.3.raw.unpack	HKTL_NET_GUID_BrowserPass	Detects c# red/black-team tools via typelibguid	Arnim Rupp (https://github.com/ruppde)	• 0x35a3:$typelibguid0: 3cb59871-0dce-453b-857a-2d1e515b0b66
7.2.CasPol.exe.37520000.3.raw.unpack	JoeSecurity_BrowserPasswordDump_1	Yara detected BrowserPassword Dump	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.11.20 - Destination IP: 158.101.44.242

Timestamp:	192.168.11.20158.101.44.24249845802039190 03/18/23-05:38:08.943594
SID:	2039190
Source Port:	49845
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected BrowserPasswordDump

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

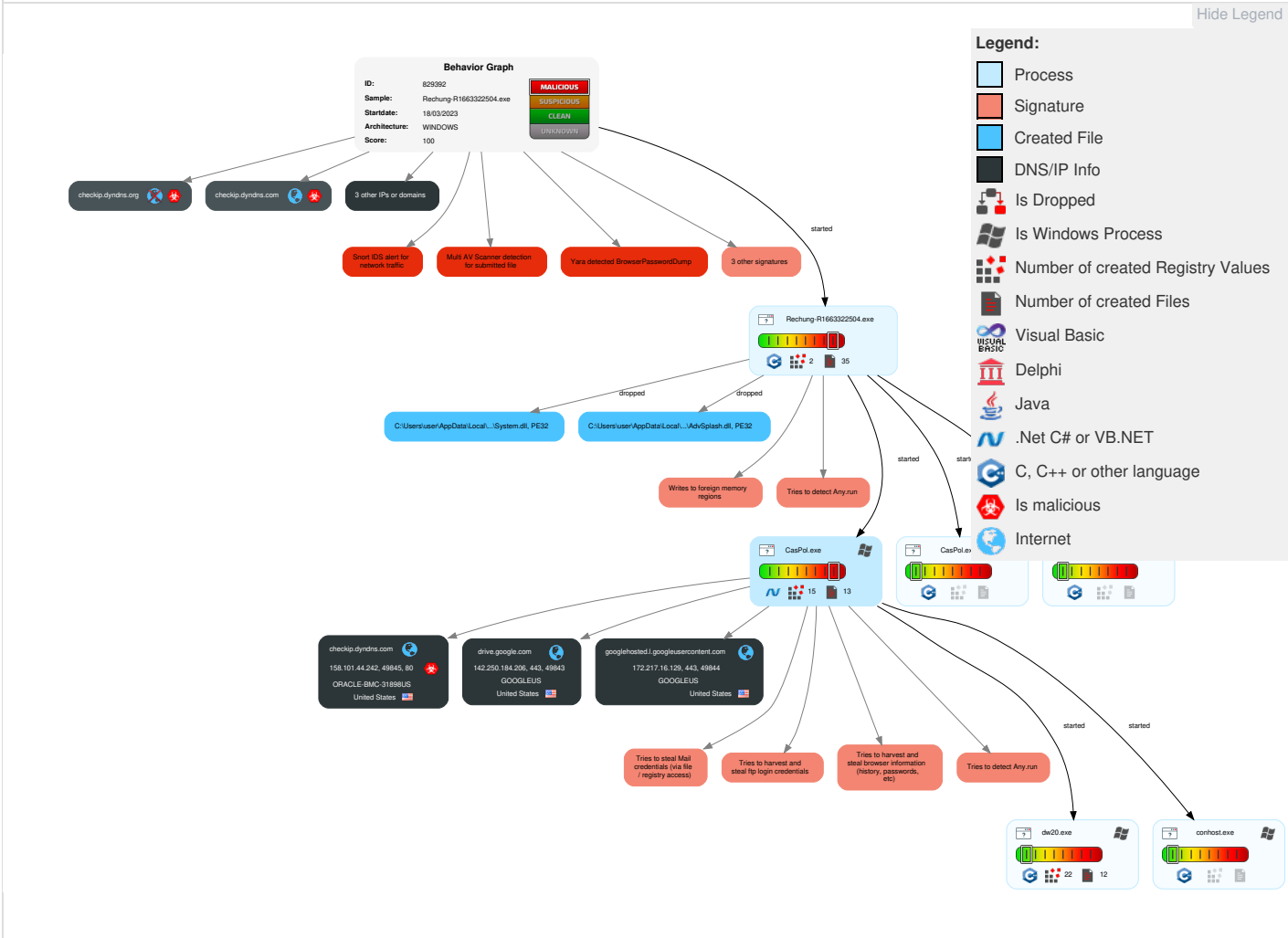
Yara detected BrowserPasswordDump

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 DLL Side-Loading	1 Access Token Manipulation	1 1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Disable or Modify Tools	Security Account Manager	1 System Network Configuration Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	4 File and Directory Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 1 Process Injection	LSA Secrets	1 6 System Information 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	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

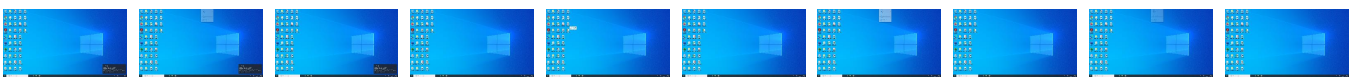
Behavior Graph

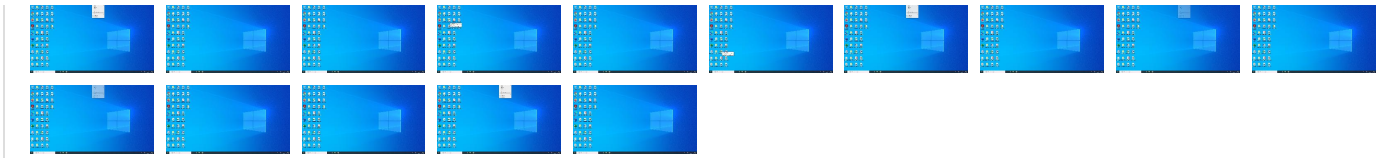


Screenshots

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
Rechung-R1663322504.exe	31%	ReversingLabs	Win32.Trojan.Tnega	
Rechung-R1663322504.exe	38%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsiF853.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsiF853.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	Virustotal		Browse
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://james.newtonking.com/projects/json	0%	Avira URL Cloud	safe	
http://crl.micros	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.184.206	true	false		high
googlehosted.l.googleusercontent.com	172.217.16.129	true	false		high
checkip.dyndns.com	158.101.44.242	true	true	• 0%, Virustotal, Browse	unknown
doc-04-c4-docs.googleusercontent.com	unknown	unknown	false		high
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

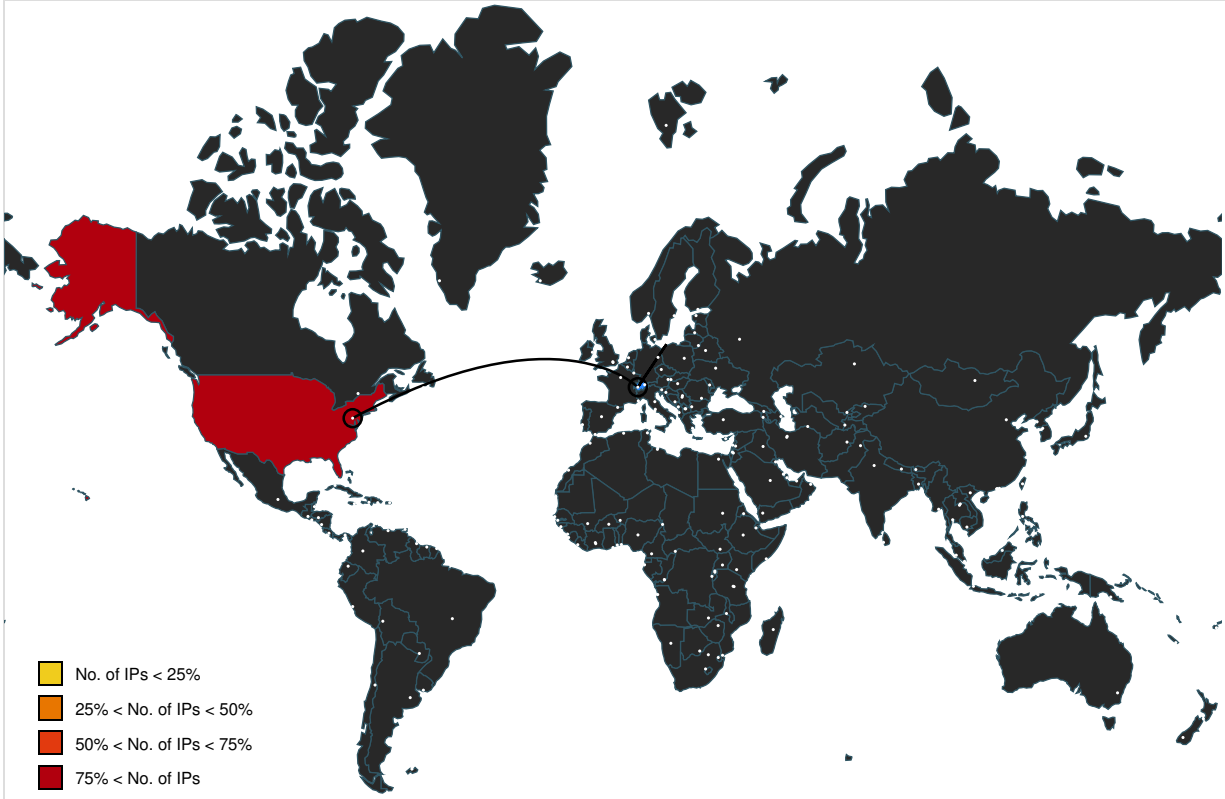
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://doc-04-c4-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/eu361v7891419i1as1r1dl2nqlomasvu/1679114250000/12853136832670220481/*/1RhzoPq21Mbz1UprqcH2DXnwFIoRgz7-I?e=download&uuid=687b7ba6-caf7-4f82-8267-8cb96e77380a	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-04-c4-docs.googleusercontent.com/	CasPol.exe, 00000007.00000002.5252241661 2.0000000004268000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 7.00000003.52345673392.00000000042C5000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.certum.pl/ctsca2021.crl0o	Rechung-R1663322504.exe	false		high
http://repository.certum.pl/ctnca.cer09	Rechung-R1663322504.exe	false		high
http://https://doc-04-c4-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/eu361v78	CasPol.exe, 00000007.00000002.5252241661 2.00000000042E0000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 7.00000003.52341294724.00000000042E4000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.52345673 392.00000000042E1000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 007.00000002.5252416612.000000000428300 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://repository.certum.pl/ctsca2021.cer0	Rechung-R1663322504.exe	false		high
http://crl.certum.pl/ctnca.crl0k	Rechung-R1663322504.exe	false		high
http://subca.ocsp-certum.com05	Rechung-R1663322504.exe	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com/	CasPol.exe, 00000007.00000002.5252241661 2.000000000422B000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://subca.ocsp-certum.com02	Rechung-R1663322504.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	Rechung-R1663322504.exe	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	Rechung-R1663322504.exe	false		high
http://repository.certum.pl/ctnca2.cer09	Rechung-R1663322504.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000007.00000002.5254052673.0000000034E46000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.microsoft.	CasPol.exe, 00000007.00000002.5256044626.0000000036F51000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://upx.sf.net	Amcache.hve.LOG1.9.dr, Amcache.hve.9.dr	false		high
http://checkip.dyndns.org	CasPol.exe, 00000007.00000002.5254052673.0000000034D71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Rechung-R1663322504.exe	false		high
http://go.microsoft.LinkId=42127	CasPol.exe, 00000007.00000002.5256044626.0000000036F51000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.certum.pl/CPS0	Rechung-R1663322504.exe	false		high
http://james.newtonking.com/projects/json	CasPol.exe, 00000007.00000002.5256188991.4.0000000037600000.00000004.08000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micros	CasPol.exe, 00000007.00000003.5234567339.2.0000000004296000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.16.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
158.101.44.242	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	true
142.250.184.206	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829392
Start date and time:	2023-03-18 05:35:01 +01:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 10m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Rechung-R1663322504.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/15@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.6% (good quality ratio 61%) • Quality average: 88% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, wdcp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many 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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_caspol.exe_5cc44e97acf31afa8e5c5ec1af53c5acde2c3_00000000_24c613c7-d23f-4749-9f08-829cc3a3e2d7\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.2686160289713344
Encrypted:	false
SSDEEP:	192:MCTLeARl7CaUaX+AMWZm9AsrMThITlui1EXuvc4Du76lfAIO82S:FeAR+aOaTMxxDu76lfAIO82
MD5:	EB6A187691ECB171BB92C9F8E305FD41
SHA1:	9BF86D62729502A98EF78F098BB6361B93D3F193
SHA-256:	EC8E0F9FC991A71C6669456807F0CD410DC40AD42C6CFDBB2D85041CF8EE476D
SHA-512:	F785180408E5E7AC0BEEA41BCA28C93E23143D08BB8C72585CC9755C76B08CD0EB9BD7CE8D721A2BD5B7828358E0DC3446EC53924E0B0810766B71CF95FF6FDE
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.2.3.5.9.1.4.9.4.6.6.7.4.2.8.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.2.3.5.9.1.4.9.5.0.1.1.1.0.7.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.4.c.6.1.3.c.7.-.d.2.3.f.-.4.7.4.9.-.9.f.0.8.-.8.2.9.c.c.3.a.3.e.2.d.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.c.a.s.p.o.l...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.6.4.-.0.0.0.1.-.0.0.1.5.-.c.7.5.4.-.c.5.c.d.5.b.5.9.d.9.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.7.9.1.2.9.a.f.7.e.f.a.4.6.2.4.4.d.a.0.6.7.6.6.0.7.2.4.2.f.0.a.6.b.7.e.1.2.e.7.8.!.C.a.s.P.o.l...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.1.9././.1.0././.2.5.:.0.8.:.5.1.:.3.4.!.2.4.3.b.5.!.C.a.s.P.o.l...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E03.tmp.WERInternalMetadata.xml

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	7620
Entropy (8bit):	3.6992698079997943
Encrypted:	false
SSDEEP:	192:R9l7lZNiWR6lhaL26Ynq6PgmfmFPXp1Qd1fYQm:R9lnNi46IIK6Yq6PgmfqTQff2
MD5:	CA48408075A231F52A067DA8CD11513C
SHA1:	025231FF1257DEAE25771552FE42E23D301AC397
SHA-256:	BC5EC16382F87B2F16A3AFBEB91E1DDD715E80C1D79B016BB3132A464A3AF2A6
SHA-512:	8C83A69466BE06D962E5760CDE9ACCC65A63355F2E71EC077F779E5CCFDAA2871928FF06045E4B193E6F4E71FE720FEF3B2B94D28E5647413707BEB8BF7EB27E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.2.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...1.1.6.5...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.1.6.5.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.2.2.0.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E62.tmp.xml

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4730
Entropy (8bit):	4.477930624054625
Encrypted:	false
SSDEEP:	48:cvIwwtl8zsYBe702l7VFJ5WS2Cfjkas3rm8M4JFKf6TF2FhO+q8wFvLB8wkd:uILfYI7GySPfIJFKEFgOtFjB8wkd
MD5:	3B2723FA6E50F304DAB44C852B06D6A3
SHA1:	584FDF4AC4D9CEED31871A830D69D8E3DE05FDC5
SHA-256:	58E37D2FBD32637D9BC03C469D6C1A071C6B09275AEC10F56FF20655397AD323
SHA-512:	C56613AD635C55E65DED3A7E109E3DF1865DD75824694AA03D56CD1A2CC4C82DD8C0D725220131FF211AE3F21049D0E305092964287063D226FB79606F2E52E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19042" />.. <arg nm="vercsdbld" val="1165" />.. <arg nm="verqfe" val="1165" />.. <arg nm="csdbld" val="1165" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="242" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="222057140" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="

C:\Users\user\AppData\Local\Temp\nsiF853.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	96:1IUNaXnnXyEIPtXvZhr5RwiULuxDtJ1+wolpE:1lx3XyEwXvZh1RwnLUDtf+I
MD5:	E8B67A37FB41D54A7EDA453309D45D97
SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E.....PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B.....

C:\Users\user\AppData\Local\Temp\nsiF853.tmp\System.dll

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8QII972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B.....

C:\Users\user\Separationerne.lnk

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:25:52 1600, mtime=Sun Dec 31 23:25:52 1600, atime=Sun Dec 31 23:25:52 1600, length=0, window=hide

Category:	dropped
Size (bytes):	1280
Entropy (8bit):	3.1309064191027343
Encrypted:	false
SSDEEP:	12:8wl0dsXUCV/tz0/CSLwrHj4/3BVYG02D23ddQ9k1MJsW+AdpiUz6AwCNfBf4t2Yi:8mrWLgD4/BV02De69kqy+pbWAZjJT
MD5:	4196863E92696387150E600E60EFC6FB
SHA1:	EB522598123ACA565CD764787F652CCAA18132CA
SHA-256:	9EE412852B59929D0F10D8647FC2F25A79C7F216578159A43B175BA544FFB4B5
SHA-512:	268236CF45F17B2D88517E753960243ECD7F402BE0D9E985929418A86D0A396C840475E8C8470A370FB894A2749A2DD2E752D54F497436B138DF76F09978694A
Malicious:	false
Preview:	L.....F.....P.O. ..i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....user..>..... .....A.r.t.h.u.r.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....\.1.... .....Microsoft.D.....M.i.c.r.o.s.o.f.t.....V.1.....Windows.@.....W.i.n.d.o.w.s.....t.1.....Printer Shortcuts.T..... .....P.r.i.n.t.e.r. .S.h.o.r.t.c.u.t.s... .t.2.....Genoptagelsen.Phi.T.....G.e.n.o.p.t.a.g.e.l.s.e.n...P.h.i... ...G...\.A.p.p.D.a.t.a.\.R.o.a.m .i.n.g.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.P.r.i.n.t.e.r. .S.h.o.r.t.c.u.t.s.\.G.e.n.o.p.t.a.g.e.l

C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Adventure_20.bmp

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, components 3
Category:	dropped
Size (bytes):	10534
Entropy (8bit):	7.884822059718216
Encrypted:	false
SSDEEP:	192:oXRZxdt62XpqRigPYtY0CfKTQlh5NKW6F5oJxfskCjGmXa6Pbplv26Zzkq:KRfdt62X+XoElh/KW6ifskEGeaIp9zkq
MD5:	A4530760E13B17372AE0D8CB48F66D0D
SHA1:	AA21564FA3A847E59402B62D3F600DDA5046A926
SHA-256:	F37F7A75DC27903EA88D1A3912DFB9123CA217E2467EB6D5DC966F60DC7F9DB7
SHA-512:	E42C32B412CD4AA560EFED98050F4B2F858190EA8BF56A81311F24C6F0751E2E397F624777E759BC80B1D34BF0AA9ECF6356E26D553D22E503A53CEF76797D4
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..9...k....X.....&.2.Z.....k~I.....e...J...}..<..M..8....."../...O.u.....5.h...71]ZZ.....v..Yc...<.i'..m2_..>..#...K...,qq.^<2\|D.V...j..ae.0Mu.^K..#k..3<."F V$HV.)..vmG..H.....z.\..#.....3_..Wo.g.>.o.....|...V.}.Ho.]...q#..W667Z`..)..I._E'.....+\.w..K....O.o..5.....4O..~.

C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	ASCII text, with very long lines (35012), with no line terminators
Category:	dropped
Size (bytes):	35012
Entropy (8bit):	2.713079331895783
Encrypted:	false
SSDEEP:	768:YOYEtjBKsUje7ciMsO9Z/mAXEEEJu+am7luxsr6mPpHOEEEEESW0ymwpTiq:d4/98AEMRNPpHrViq
MD5:	F75A78EE11492D9F9146075023D485D3
SHA1:	772AE864C11AE2C45834F681EFDF662BBD28268B
SHA-256:	5916C8773319EA24B225C76FE361D360360CE03E1F61E2E86387514A185BDAF9
SHA-512:	BB2D74E9F7D7F02E682E302B115C280C886F4E99789F4E5A198E7B2E973FFBE788559140CC2625EE8F754831497E67038CA327196EC14370968B47828863BD0D
Malicious:	false
Preview:	0000000000000F00007200F400C000D900DDDD00009D005D5D5D000E0E0E0E00C20000005F5F5F00E4E4E400000000009B0013000026262600A90000 8C006D00323200360000001717008700C600B4B400007900B0B0B0B0000000006F6F004C4C00590000003F000041414100004C00C1C1C1C10000004A4A00000000AA AA0000000000F10039390000000004300000AC00F6000093002600C5C5000000002900006700002C000000AE000000670001000000000004D005D5D5D0000E0E00046 46464600C90000202000D8000086005700BDBD00007000212100FC000606060600080068000000000D8D800A700006060009200A4004600D000CCCC00E9E90000 005700F600888888002700CCCC00000000006F6F00D9003D3D3D009F000000000000DDDDDD0000B2000000001B0000CD003D3D000606060055D5D0000 B5B5B5B5009898007100DE000F000000F0F0F000BDBD000000000012121200000048000E1003A3A3A00565656000000000B60000000013002727270 0E90000000096 96004B00770078000000A8000000DCDC0007070700C8005959595959000D000000840000740000EAEA00D9D9D9D900000000A70000B70000828282820000780082 8200000000000000515151007878000022220008E0000DB00001E0000DD006C00FA00000000AAAA0000009500000025 00CF00000000A000

C:\Users\user\Socialdirektrer\Vandspildets.Shi37

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	data
Category:	dropped
Size (bytes):	225168
Entropy (8bit):	7.3676127973119225

Encrypted:	false
SSDEEP:	3072:NOUzxidFkCI6+rXNfJEow2a5KTa49D1bdzeDZ/7SkPtnWpA2Or1/nD9kS/fmi:s9dFrl6ifJLwV0/9Jd4RSYtWpBanD9kG
MD5:	BAFC11E1543369B58D7852857D986EFA
SHA1:	A00AD13ECA7F98C1CBBC7AE32151D3878DD2BBB0
SHA-256:	F8D1014289006D2ACCAB3D5A1C36CD867B4D6BEC50781365175B4FF8323A5E81
SHA-512:	69883FDF36A90C35625D74BF7FE5808AFD1F88314EF60FAB7785C443BD992F72656BB727E3E44503266BECC28A48E0BAF7DF70A6C5CAA10D2B2DFED28C07AA02
Malicious:	false
Preview:	.....t..cc.....dd.@@.rr..ZZ.====.....vvvvv.""...i..SS.....((.v.....dd.....K.....m.....OO.....@@.....00._..... ...XX...EE..$$.HHHHHH.....m.....nn.....oo.....hhh.....__.....^.7.....#.....1..-.....H...J.....???.....|..>.^.W..... .....H..^^^^^^..???.CCC..n.....nnn.xx.....;.....E.....&&&&.....hhh....W.....?.ss....B.b....III.....#.....q.....Q.s...#... .....%...nn.EE.....||.....___.....p.....R.88.....$.....LL.....k.....I...".pp.....:.aa.....].....&.....jj..`.JJ.....//.... e...^^^^^^^^^^....2.p.....I.....$.....oo.....E.....

C:\Users\user\Socialdirektrer\media-floppy-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	183
Entropy (8bit):	6.337608034945541
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllTV00EDgZ1uP6he3LFIY8roNQh/e9OuTB+Mg1J7d:6v/lhPysY0EeDyLiRroCh/0B+v1MC1jp
MD5:	293D1D4F18C3A918A44FAD289715E950
SHA1:	BD92A45835DD693FE8D0B72F296FE0134D46B876
SHA-256:	553F673950BE4DE71377A297050888D0BE5A997DB334781994C3265EDA30C7B3
SHA-512:	E62D45E30997EB18EB3C45BC1574C75462DC4CC36144D4E529F917B6091ADD14F91779F5C428458CEA129EF37B27FDDBBCEA8E5005563DC2AABCB370BEDF2E8C
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....nIDAT8.....0...wp(.....,...J.A[.O....i.4..x d..F.(.N.$ .su.w.C.~..XyZ.|.....k....z`../..aA.<.>....j.. ...=....z....IEND.B`.

C:\Users\user\Socialdirektrer\mk.txt

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	8934
Entropy (8bit):	4.259244159879149
Encrypted:	false
SSDEEP:	192:ia3g0F7SHayJ5vKVEB3Bxg5GteGIxpWNMll39oWvt/i4drxJ4MrZEXSW:iWg0zyJlKVEB3A6SM2mWvt/i4dtJ4MNO
MD5:	71D42ABE45803AC9C3DA5FCACF9CC59C
SHA1:	98A1049906972ABB480ABAF1F5658C1B8C10F27C
SHA-256:	78F5CB9345AB258CF745EAA90D44C7A7A73D3FE06EA182B1298A989135FFA11F
SHA-512:	A0096575D6F911CC2600DAC93D6FD7AA8D9E2F9F71A92571A76996FB4C47BDB714BBA453C862B3F42CC5F4BAAF2AED1DFF3C9D6F84A3E2053FF2037C56AB85A5
Malicious:	false
Preview:	.;|@Lang2@!UTF-8!..; 4.09 : Gabriel Stojanoski..;..;..;..;..;..;..;..;..;..;..0..7-Zip..Macedonian.....401.....&....&....&.....&.....440.... &..... .&..... .....&.....&.....&..... ....?..500..&.....&.....&.....&.....&.....540..&..... &..... &.....&.....&.....&.....&..... .....&. ....&.....&..... .....&..... .....&.....&..... ....&.....600..... &..... ...

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	2359296
Entropy (8bit):	4.229686725490386
Encrypted:	false
SSDEEP:	24576:o8pJ5yNYJkymnjNS1O2k5cTBagmcnYJA:o8pJ5yNYJkymnjNQA5mBagmcnYJA
MD5:	327F109CCA4114DE4FE63066D46805A7
SHA1:	3798C39C38008FB918DCB98DF7DC3C54EC4B17C5
SHA-256:	9D4022C4B5D40785C0B700F710E7F9FBFD14BDAAE9613FE4ACCCDF6BF253BD65
SHA-512:	EF221FA284132C8638A02BDE73FE05AAF6FBD9F32073947FFD5D9B4680B979DD7BADD816B121BACC6BA53081623163C41DA0CF7C7B9419E5C8C51ECE839CF65
Malicious:	false

Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm...OY..... ....}.{}..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	376832
Entropy (8bit):	2.6371963290907305
Encrypted:	false
SSDEEP:	3072:fpFZfwN1/HecetetUuM/aNim4ixiyuiKisiXiPG7ieCNi5gU5zH35Gs3MOx02EnC:fvZoN1vJAO84iTd+v4He3TKz
MD5:	8726C4CBDA130722A758F76728527B19
SHA1:	7E989D5E29BECA70895BF7F8DCE7ECD5A502B331
SHA-256:	3856E2E2811C31B7CFB6872DB96F0E384ECA9C3B6DDE5B9712BFC85D20A2B952
SHA-512:	BBF5D267ABC9A6C2A8750B14901D56840CFD00473125732250EB2C22B0F0EA0A4756B30B090A9F182EDFD2F5C0EE862F8DD74CFE66C79378D4DB416DA05CB94
Malicious:	false
Preview:	regf.....5.#.^..... ....P .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e.....Q.....P..#....Q.....P..#.....Q.....P..#.rmtm...OY..... ....{.{}HvLE.....P ...../.E..d)H."..... .....@.....@..... ....hbin.....5.#.^.....nk,....S..... ....&...{11517B7C-E79D-4e20-961B-75A811715ADD}.....nk ...k.PY.....(.....@.....*...N.....)...InventoryMiscellaneousMemorySlotArray Info.....mG.....nk .$4./T..... .....

C:\Windows\assembly\Desktop.ini

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	Windows desktop.ini
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.2735028737400205
Encrypted:	false
SSDEEP:	6:a1eZBXVNYTF0NwoScUbtSgyAXIWv7v5PMKq:UeZBFNYTswUq1r5zq
MD5:	F7F759A5CD40BC52172E83486B6DE404
SHA1:	D74930F354A56CFD03DC91AA96D8AE9657B1EE54
SHA-256:	A709C2551B8818D7849D31A65446DC2F8C4CCA2DCBBC5385604286F49CFDAF1C
SHA-512:	A50B7826BFE72506019E4B1148A214C71C6F4743C09E809EF15CD0E0223F3078B683D203200910B07B5E1E34B94F0FE516AC53527311E2943654BFCEADE53298
Malicious:	false
Preview:	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==..[.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	158
Entropy (8bit):	4.298534139898036
Encrypted:	false
SSDEEP:	3:WNEDkFrA7fwkh07NfORRAzs2VkNatO3MLlDKlEsExLrWwrAXTcFrXX8:WsTbRh07NkMswksKML4lOBWEylFrc
MD5:	95A9765293B395853C7059AB01DA28AE
SHA1:	7627EBC68CCE94B1E1CCC826C0D14D8068B3C90D
SHA-256:	08E334353322F44FDC19102929B367F4D870F3BC8872F973EAAA8119B6AC771F
SHA-512:	47D1F81B3E26D4BC20954268285ACE3DAA970A5B78F3E6F31BF8266F2310702B57CDF285839BACE9635BE31A2479F9126814FFA4E832C2864080A9C8918D9505
Malicious:	false
Preview:	.Unhandled Exception: System.AccessViolationException: Attempted to read or write protected memory. This is often an indication that other memory is corrupt..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.1116261135004395
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Rechung-R1663322504.exe
File size:	416280
MD5:	11b5b208de7a85b46104a0597c5da7dc
SHA1:	c578bc317e666159cbfc191cb4e50de2de03ab79
SHA256:	0a80ba418f561098477e18cc42ddfc31796b2be3166ff6c99967b98388fe4826
SHA512:	c79e0deeb1686edc5bfe2db026f423277740fe816a674a3111fb36fd4813825a080048b44d03e92310db526a8c791259684778f8dea0861cd9b26e2f5f0b5d23
SSDEEP:	6144:16bAcJtT+SdoujpZM5DMJ+VGM1IMwJ1OPH7USLahNcfM9rQ09j3V/PySssz:2APSbyDMOJrOPH7UfnpCSD
TLSH:	B694BFA0F620D0DADCB417F16C9FD9211AE76EECE4E0220F65A73259AD736D3051F24A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d....:....

File Icon

Icon Hash:	f169e8e4e4ccca88

Static PE Info

General

Entrypoint:	0x403350
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759518 [Mon Jul 24 06:35:04 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Departmentalizations@Trisulphide193.Lok, OU="Pasteuriseringens Eternellerne ", O=Stikprvestandardafvigelsernes, L=Dividing Creek, S=New Jersey, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 27/12/2022 11:19:02 26/12/2025 11:19:02
Subject Chain	• E=Departmentalizations@Trisulphide193.Lok, OU="Pasteuriseringens Eternellerne ", O=Stikprvestandardafvigelsernes, L=Dividing Creek, S=New Jersey, C=US
Version:	3
Thumbprint MD5:	1F7F4BF42A830708AC95921509004FCC
Thumbprint SHA-1:	54B3D870C522C1CA544E3D38597EEC9DC6D3C3A0
Thumbprint SHA-256:	ED0BD8E407BDD2EB9D4B7BDFEC49D761B0F85D212BDFDC1A3F9981BBA4AD638B
Serial:	4122AFC051A99F02AE188FBC961AC5C36F876297

Entrypoint Preview

Instruction
sub esp, 000002D4h

Instruction
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007F40DCB82EE3h
push ebx
call 00007F40DCB86179h
cmp eax, ebx
je 00007F40DCB82ED9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F40DCB860F3h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F40DCB82EBCh
push 0000000Ah
call 00007F40DCB8614Ch
push 00000008h
call 00007F40DCB86145h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007F40DCB86139h
cmp eax, ebx
je 00007F40DCB82EE1h
push 0000001Eh
call eax
test eax, eax
je 00007F40DCB82ED9h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d3000	0x281f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x63778	0x22a0	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.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	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x2a000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3d3000	0x281f0	0x28200	False	0.35579731308411217	data	5.085440369030725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d3310	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x3e3b38	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x3ecfe0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x3f2468	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x3f6690	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x3f8c38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x3f9ce0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x3fa668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x3faad0	0x120	data	English	United States
RT_DIALOG	0x3fabf0	0x11c	data	English	United States
RT_DIALOG	0x3fad10	0xc4	data	English	United States
RT_DIALOG	0x3fadd8	0x60	data	English	United States
RT_GROUP_ICON	0x3fae38	0x76	data	English	United States
RT_MANIFEST	0x3faeb0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

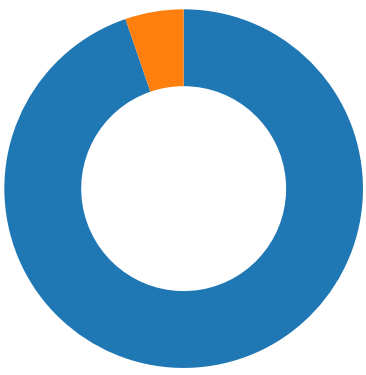
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20158.101.44.24249845802039190 03/18/23-05:38:08.943594	TCP	2039190	ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49845	80	192.168.11.20	158.101.44.242

Network Port Distribution



Total Packets: 57

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:38:07.192332983 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.192359924 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.192634106 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.205848932 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.205863953 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.243274927 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.243577957 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.244079113 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.244271040 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.301903009 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.303085089 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.303307056 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.306361914 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.348496914 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.686002016 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.686170101 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.686347961 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.686557055 CET	443	49843	142.250.184.206	192.168.11.20
Mar 18, 2023 05:38:07.686769009 CET	49843	443	192.168.11.20	142.250.184.206
Mar 18, 2023 05:38:07.791002989 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.791033030 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.791369915 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.791657925 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.791678905 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.834359884 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.834547997 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.834606886 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.835166931 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.835330009 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.835330009 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.838656902 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.838684082 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.839046001 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:07.839221954 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.839565992 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:07.880487919 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.059297085 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.059484959 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.059570074 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.059582949 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.059621096 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.059700012 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.059746981 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.059823990 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.061012030 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.061258078 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.061803102 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.062004089 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.062004089 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.062004089 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.062088013 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.062323093 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.063960075 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.064158916 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.064220905 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.064448118 CET	49844	443	192.168.11.20	172.217.16.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:38:08.066956043 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.067177057 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.067687035 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.067857027 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.067909002 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.068015099 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.068114996 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.068186998 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.068217993 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.068413973 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.068625927 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.068834066 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.068902969 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.069087982 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.069444895 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.069610119 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.069678068 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.069844007 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.070167065 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.070367098 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.070437908 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.070699930 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.070875883 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.071058989 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.071125031 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.071337938 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.071608067 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.071770906 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.071839094 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.072031021 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.072288036 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.072453976 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.072556973 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.072715998 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.072776079 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.072920084 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.073020935 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.073086023 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.073132038 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.073306084 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.073761940 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.073991060 CET	49844	443	192.168.11.20	172.217.16.129
Mar 18, 2023 05:38:08.073998928 CET	443	49844	172.217.16.129	192.168.11.20
Mar 18, 2023 05:38:08.074049950 CET	443	49844	172.217.16.129	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 05:38:07.178211927 CET	60445	53	192.168.11.20	1.1.1.1
Mar 18, 2023 05:38:07.187526941 CET	53	60445	1.1.1.1	192.168.11.20
Mar 18, 2023 05:38:07.758445024 CET	63232	53	192.168.11.20	1.1.1.1
Mar 18, 2023 05:38:07.789558887 CET	53	63232	1.1.1.1	192.168.11.20
Mar 18, 2023 05:38:08.780349016 CET	65013	53	192.168.11.20	1.1.1.1
Mar 18, 2023 05:38:08.789386034 CET	53	65013	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 18, 2023 05:38:07.178211927 CET	192.168.11.20	1.1.1.1	0xe0f5	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:07.758445024 CET	192.168.11.20	1.1.1.1	0xaebb	Standard query (0)	doc-04-c4-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.780349016 CET	192.168.11.20	1.1.1.1	0xce36	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

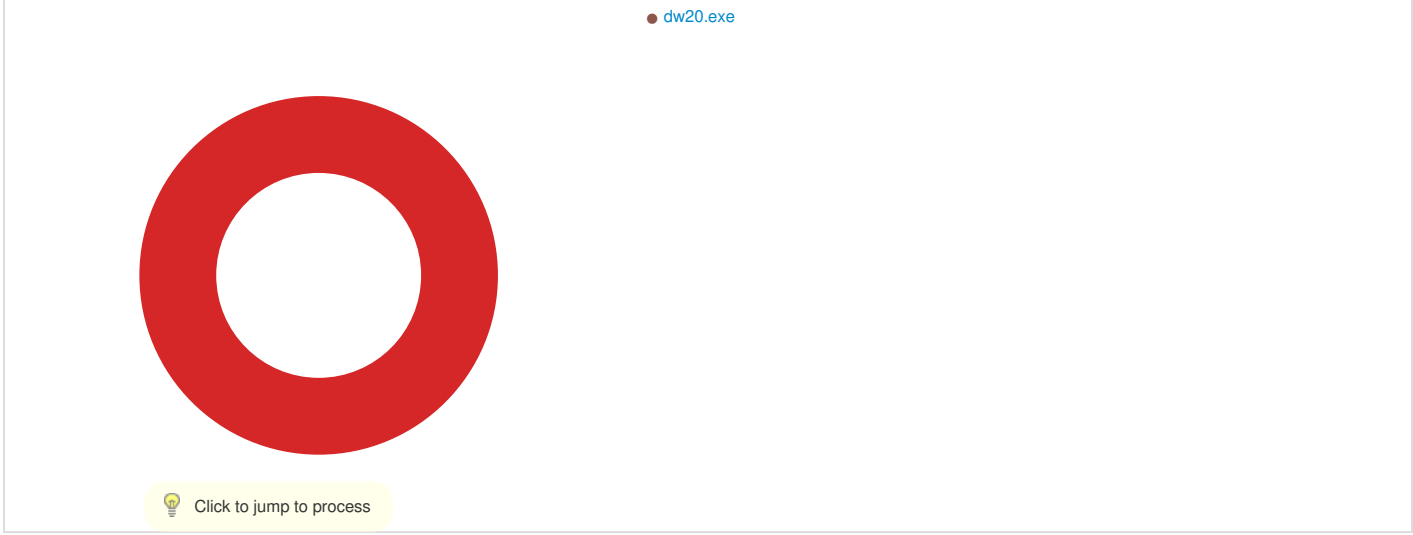
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 18, 2023 05:38:07.187526941 CET	1.1.1.1	192.168.11.20	0xe0f5	No error (0)	drive.google.com		142.250.184.206	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:07.789558887 CET	1.1.1.1	192.168.11.20	0xaebb	No error (0)	doc-04-c4-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 18, 2023 05:38:07.789558887 CET	1.1.1.1	192.168.11.20	0xaebb	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.129	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Mar 18, 2023 05:38:08.789386034 CET	1.1.1.1	192.168.11.20	0xce36	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-04-c4-docs.googleusercontent.com
- checkip.dyndns.org

Statistics

Behavior



System Behavior

Analysis Process: Rechung-R1663322504.exe PID: 6340, Parent PID: 4988

General

Target ID:	1
Start time:	05:36:55
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Imagebase:	0x400000
File size:	416280 bytes
MD5 hash:	11B5B208DE7A85B46104A0597C5DA7DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.52371090291.000000000690B000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **6560**, Parent PID: **6340**

General	
Target ID:	5
Start time:	05:38:01
Start date:	18/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Imagebase:	0xd0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **3312**, Parent PID: **6340**

General	
Target ID:	6
Start time:	05:38:01
Start date:	18/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Imagebase:	0x490000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **5220**, Parent PID: **6340**

General	
Target ID:	7
Start time:	05:38:01
Start date:	18/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Imagebase:	0xcb0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: HKTL_NET_GUID_BrowserPass, Description: Detects c# red/black-team tools via typelibguid, Source: 00000007.00000002.52561610808.0000000037520000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp (https://github.com/ruppde) • Rule: JoeSecurity_BrowserPasswordDump_1, Description: Yara detected BrowserPasswordDump, Source: 00000007.00000002.52561610808.0000000037520000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BrowserPasswordDump_1, Description: Yara detected BrowserPasswordDump, Source: 00000007.00000002.52540526737.0000000034E8C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BrowserPasswordDump_1, Description: Yara detected BrowserPasswordDump, Source: 00000007.00000002.52560446262.0000000036F71000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BrowserPasswordDump_1, Description: Yara detected BrowserPasswordDump, Source: 00000007.00000002.52540526737.0000000034E46000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.52540526737.0000000034D71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32CC380	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD3614C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD3614C	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD3614C	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD3614C	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\assembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CFE1F27	unknown
C:\Windows\assembly\Desktop.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CFE1F27	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\assembly\Desktop.ini	0	227	3b 20 3d 3d 2b 2b 3d 3d 0d 0a 3b 20 0d 0a 3b 20 20 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 3b 20 0d 0a 3b 20 3d 3d 2d 2d 3d 3d 0d 0a 5b 2e 53 68 65 6c 6c 43 6c 61 73 73 49 6e 66 6f 5d 0d 0a 43 4c 53 49 44 3d 7b 31 44 32 36 38 30 43 39 2d 30 45 32 41 2d 34 36 39 64 2d 42 37 38 37 2d 30 36 35 35 35 38 42 43 37 44 34 33 7d 0d 0a 43 6f 6e 66 69 72 6d 46 69 6c 65 4f 70 3d 31 0d 0a 49 6e 66 6f 54 69 70 3d 43 6f 6e 74 61 69 6e 73 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 73 74 61 62 69 6c 69 74 79 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0d 0a	; ==++==; ; Copyright (c) Microsoft Corporation. All rights reserved.; ; ==--==[.ShellClassInfo]CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}ConfirmFileOp=1InfoTip=Contains application stability information.	success or wait	1	6CFE1F27	unknown
\Device\ConDrv	1	1	55	U	success or wait	1	6CF79D39	WriteFile
\Device\ConDrv	21	20	20 53 79 73 74 65 6d 2e 41 63 63 65 73 73 56 69 6f 6c 61 74	System.AccessViolat	success or wait	1	6CF79D39	WriteFile
\Device\ConDrv	22	1	53	S	success or wait	1	6CF79D39	WriteFile
\Device\ConDrv	157	135	0a		success or wait	1	6CF79D39	WriteFile
\Device\ConDrv	158	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CF79D39	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6CD687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6CD687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CD687D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	34B6B7DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	34B6B7DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	34B6B7DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	34B6B7DB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	34B6B7DB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	34B6B7DB	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	6CD655E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	6CD655E4	unknown
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	34B6B7DB	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5764**, Parent PID: **5220**

General

Target ID:	8
Start time:	05:38:01
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ee940000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: dw20.exe PID: **9028**, Parent PID: **5220**

General

Target ID:	9
Start time:	05:38:14
Start date:	18/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2584
Imagebase:	0x10000000
File size:	36264 bytes
MD5 hash:	89106D4D0BA99F770EAFE946EA81BB65
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly

No disassembly