ID: 680518
Sample Name: JULY SOA.exe
Cookbook: default.jbs
Time: 18:19:05
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

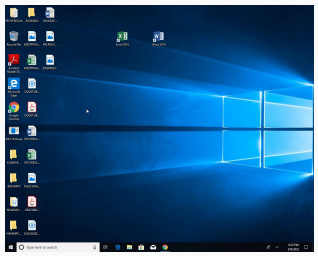
Windows Analysis Report

JULY SOA.exe

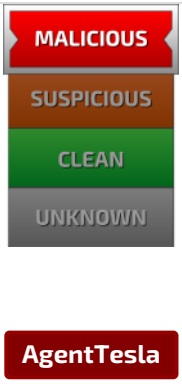
Overview

General Information

Sample Name:	JULY SOA.exe
Analysis ID:	680518
MD5:	c059fd1e2ec2df2..
SHA1:	5cfadf7c2097145..
SHA256:	6c9947dd57c1a9..
Tags:	agenttesla exe
Infos:	



Detection



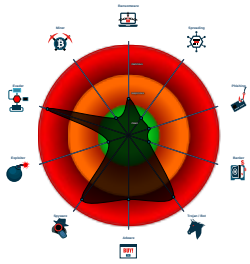
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…

Classification



Process Tree

- **System is w10x64**
- JULY SOA.exe (PID: 5808 cmdline: "C:\Users\user\Desktop\JULY SOA.exe" MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
  - schtasks.exe (PID: 2232 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qOHVWexsnI" /XML "C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - JULY SOA.exe (PID: 5668 cmdline: {path} MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
  - JULY SOA.exe (PID: 4588 cmdline: {path} MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
  - JULY SOA.exe (PID: 4972 cmdline: {path} MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
- DnDcR.exe (PID: 2080 cmdline: "C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe" MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
  - schtasks.exe (PID: 5508 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qOHVWexsnI" /XML "C:\Users\user\AppData\Local\Temp\tmp158E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DnDcR.exe (PID: 5900 cmdline: {path} MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
  - DnDcR.exe (PID: 3896 cmdline: {path} MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
- DnDcR.exe (PID: 3168 cmdline: "C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe" MD5: C059FD1E2EC2DF2B8E4AF62359868B1B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "francisco@palumalimited.com",
  "Password": "+D&GRBh14#(M",
  "Host": "mail.palumalimited.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x1e5640:$a13: get_DnsResolver • 0x2f2e80:$a13: get_DnsResolver • 0x1e3e4f:$a20: get_LastAccessed • 0x2f168f:$a20: get_LastAccessed • 0x1e5fbe:$a27: set_InternalServerPort • 0x2f37fe:$a27: set_InternalServerPort • 0x1e62da:$a30: set_GuidMasterKey • 0x2f3b1a:$a30: set_GuidMasterKey • 0x1e3f56:$a33: get_Clipboard • 0x2f1796:$a33: get_Clipboard • 0x1e3f64:$a34: get_Keyboard • 0x2f17a4:$a34: get_Keyboard • 0x1e525b:$a35: get_ShiftKeyDown • 0x2f2a9b:$a35: get_ShiftKeyDown • 0x1e526c:$a36: get_AltKeyDown • 0x2f2aac:$a36: get_AltKeyDown • 0x1e3f71:$a37: get_Password • 0x2f17b1:$a37: get_Password • 0x1e4a0b:$a38: get_PasswordHash • 0x2f224b:$a38: get_PasswordHash • 0x1e5a40:$a39: get_DefaultCredentials
00000013.00000002.450194726.0000000004362000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.450194726.0000000004362000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Click to see the 22 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
16.0.JULY SOA.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.0.JULY SOA.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
16.0.JULY SOA.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c57:$s10: logins • 0x326be:$s11: credential • 0x2eca6:$g1: get_Clipboard • 0x2ecb4:$g2: get_Keyboard • 0x2ecc1:$g3: get_Password • 0x2ff9b:$g4: get_CtrlKeyDown • 0x2ffab:$g5: get_ShiftKeyDown • 0x2ffbc:$g6: get_AltKeyDown
16.0.JULY SOA.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30390:$a13: get_DnsResolver • 0x2eb9f:$a20: get_LastAccessed • 0x30d0e:$a27: set_InternalServerPort • 0x3102a:$a30: set_GuidMasterKey • 0x2eca6:$a33: get_Clipboard • 0x2ecb4:$a34: get_Keyboard • 0x2ffab:$a35: get_ShiftKeyDown • 0x2ffbc:$a36: get_AltKeyDown • 0x2ecc1:$a37: get_Password • 0x2f75b:$a38: get_PasswordHash • 0x30790:$a39: get_DefaultCredentials
19.2.DnDcR.exe.43cbec8.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 28 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

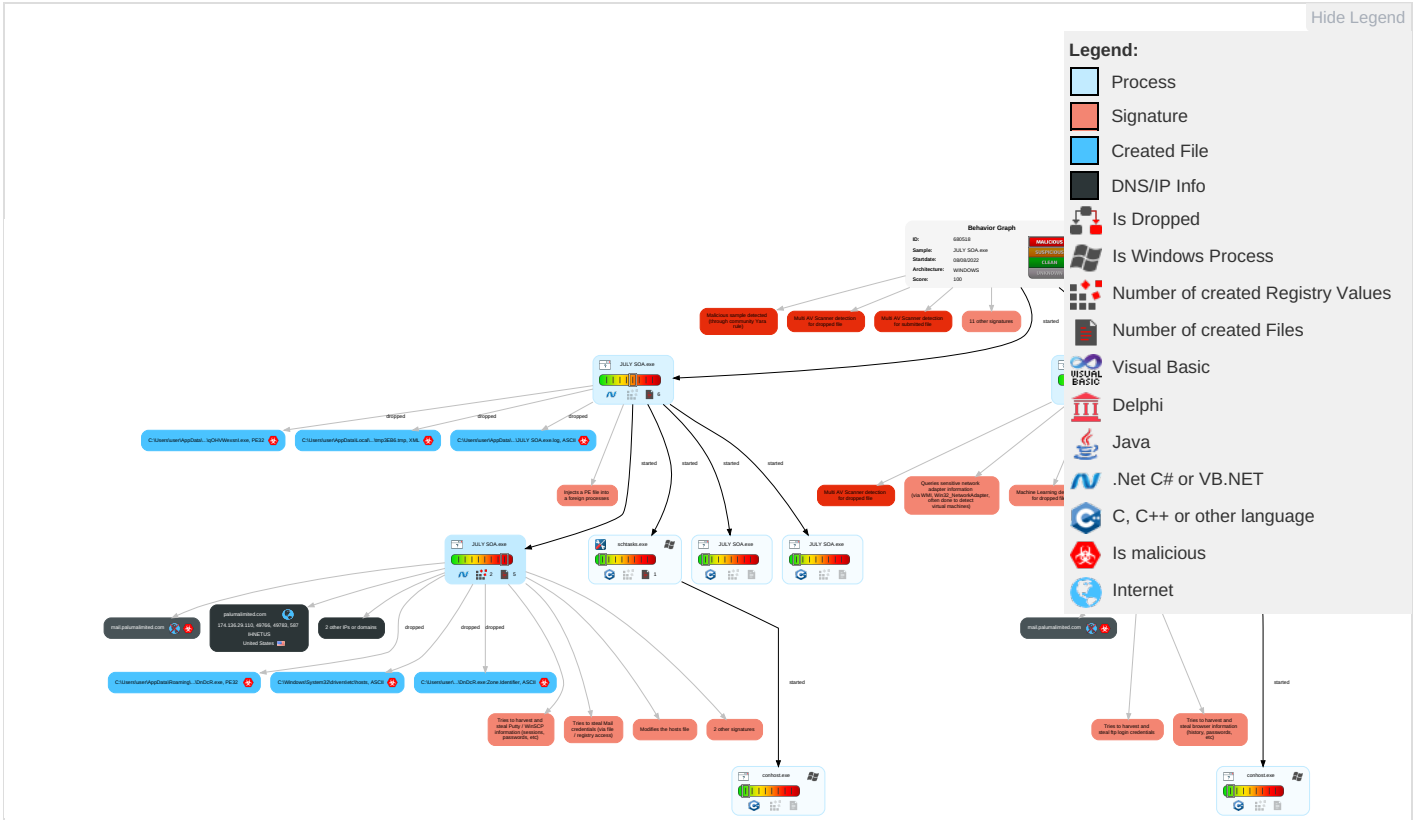
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	2 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 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)	2 Obfuscated Files or Information	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	1 Process 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	1 Masquerading	Cached Domain Credentials	1 4 1 Virtualization/Sandbox Evasion	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 4 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

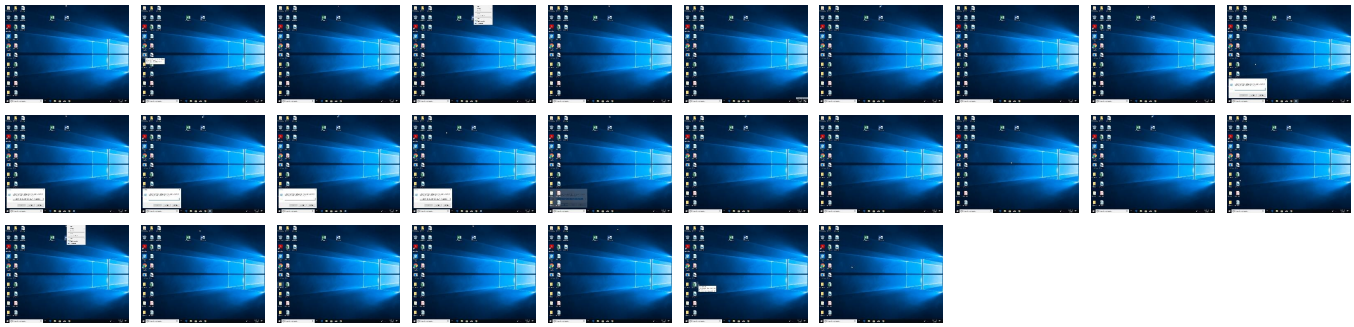
Behavior Graph



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
JULY SOA.exe	59%	Virustotal		Browse
JULY SOA.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
JULY SOA.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\qOHVWexsnI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
C:\Users\user\AppData\Roaming\qOHVWexsnI.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.JULY SOA.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
palumalimited.com	2%	Virustotal		Browse
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse
mail.palumalimited.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.fontbureau.comd=	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.tiro.comco	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.sandoll.co.krt	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://www.sandoll.co.krq	0%	Avira URL Cloud	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://www.fontbureau.comcomaF	0%	Avira URL Cloud	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-ez	0%	Avira URL Cloud	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://mail.palumalimited.com	0%	Avira URL Cloud	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	URL Reputation	safe	
http://www.rcsc.lt/repository0	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comF6	0%	Avira URL Cloud	safe	
http://www.carterandcone.comyle	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crt08	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fonts.comx	0%	URL Reputation	safe	
http://www.fontbureau.comsiva	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	URL Reputation	safe	
http://www.oaticerts.com/repository.	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://www.fontbureau.comTTFq	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://www.founder.com.cn/cni:	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	0%	URL Reputation	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://crl.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	0%	URL Reputation	safe	
http://www.fontbureau.comdsed	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-e	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
palumalimited.com	174.136.29.110	true	false	• 2%, Virustotal, Browse	unknown
windowsupdatebg.s.llnwi.net	178.79.225.128	true	false	• 0%, Virustotal, Browse	unknown
mail.palumalimited.com	unknown	unknown	true	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	JULY SOA.exe, 00000010.00000003.38795382 0.0000000006178000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	JULY SOA.exe, 00000010.00000003.39099340 2.0000000006BD5000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd=	JULY SOA.exe, 00000000.00000003.26750278 2.0000000005A7A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000003.267065355.0000000005A79000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.dhimyotis.com/certignarootca.crl0	JULY SOA.exe, 00000010.00000003.38795382 0.0000000006178000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.chambersign.org1	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.390634314.0000000006156000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.390070081.000000 0006174000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.swisssign.com/0	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.000000 0006159000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://www.fontbureau.com/designers	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	JULY SOA.exe, 00000010.00000003.39114900 6.0000000006C40000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	JULY SOA.exe, 00000010.00000002.53233598 8.0000000000E8C000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	JULY SOA.exe, 00000010.00000002.53233598 8.0000000000E8C000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comco	JULY SOA.exe, 00000000.00000003.26047861 9.0000000005A8B000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	JULY SOA.exe, 00000000.00000002.31358397 3.00000000029F1000.00000004.00000800.000 20000.00000000.sdmp, DnDcR.exe, 00000013 .00000002.434546929.00000000032A1000.000 00004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%	JULY SOA.exe, 00000010.00000002.53544055 1.0000000002A41000.00000004.00000800.000 20000.00000000.sdmp, DnDcR.exe, 0000001B .00000002.536397827.00000000030C1000.000 00004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://pki.registradores.org/normativa/index.htm0	JULY SOA.exe, 00000010.00000003.38838615 8.0000000006C41000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://policy.camerfirma.com0	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.000000 0006159000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	JULY SOA.exe, 00000010.00000002.56310974 4.0000000006121000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	JULY SOA.exe, 00000010.00000003.39074739 7.0000000006122000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.390243547.0000000006149000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000 000611C000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	JULY SOA.exe, 00000010.00000002.56250578 3.00000000060F1000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000002.551057155.0000000002D9E000. 00000004.00000800.00020000.00000000.sdmp, DnDcR.exe, 0000001B.00000002.551678919 .000000000341A000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krt	JULY SOA.exe, 00000000.00000003.26136410 6.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	JULY SOA.exe, 00000010.00000002.56325392 2.000000000616E000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.000000 0006159000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	JULY SOA.exe, 00000010.00000003.39074739 7.0000000006122000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krq	JULY SOA.exe, 00000000.00000003.26136410 6.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://wwww.certigna.fr/autorites/0m	JULY SOA.exe, 00000010.00000003.38795382 0.0000000006178000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	JULY SOA.exe, 00000010.00000002.53544055 1.0000000002A41000.00000004.00000800.000 20000.00000000.sdmp, DnDcR.exe, 0000001B .00000002.536397827.00000000030C1000.000 00004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	JULY SOA.exe, 00000010.00000002.56310974 4.0000000006121000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.390070081.0000000006174000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.390070081.0000000006174000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comcomaF	JULY SOA.exe, 00000000.00000003.26706535 5.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

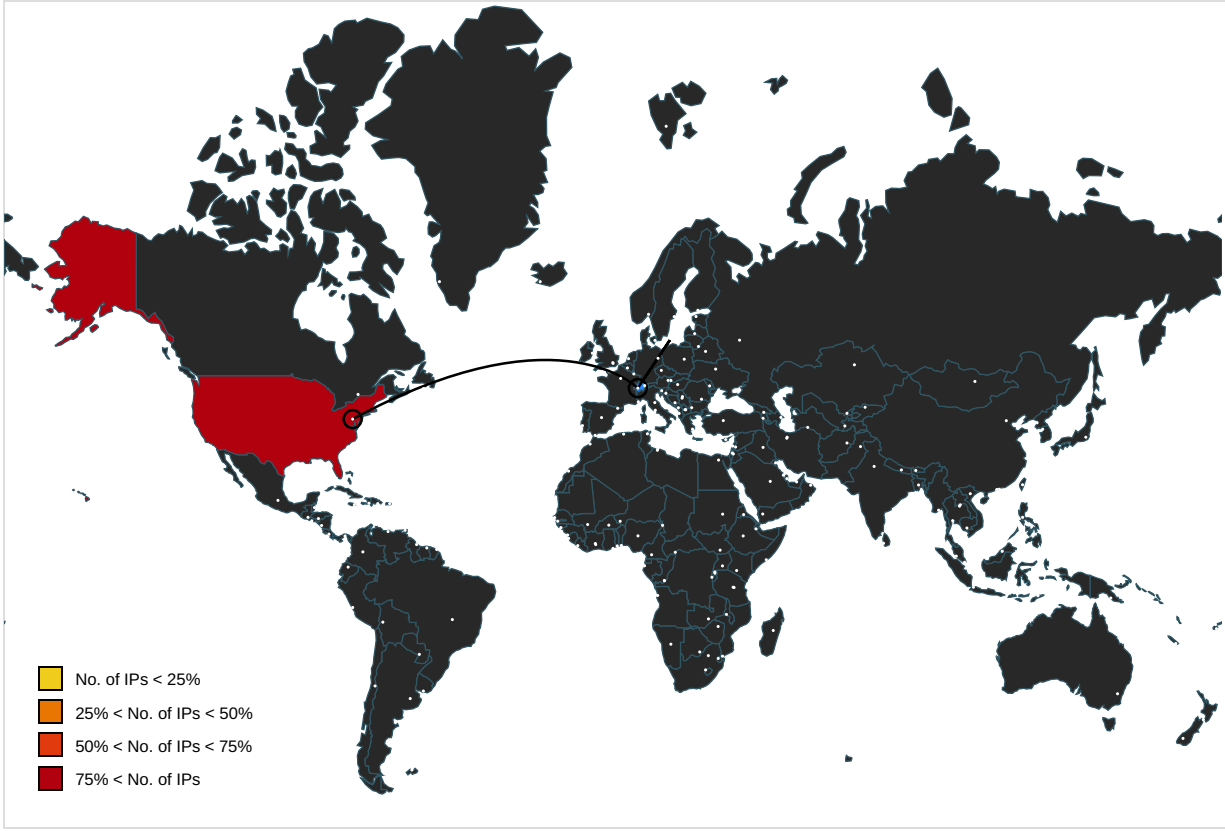
Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.oces.trust2408.com/oces.crl0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://certs.oaticerts.com/repository/OATICA2.crl	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	JULY SOA.exe, 00000010.00000003.39068701 3.0000000006158000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.390243547.0000000006149000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000 000611C000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.000000 0006159000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cns-ez	JULY SOA.exe, 00000000.00000003.26219897 8.0000000005AAD000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org0	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.palumalimited.com	JULY SOA.exe, 00000010.00000002.55105715 5.0000000002D9E000.00000004.00000800.000 20000.00000000.sdmp, DnDcR.exe, 0000001B .00000002.551678919.000000000341A000.000 00004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.firmaprofesional.com/cps0	JULY SOA.exe, 00000010.00000003.39074739 7.0000000006122000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000002.563149008.0000000006133000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000 000611C000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://www.agesic.gub.uy/acrn/acrn.crl0)	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF6	JULY SOA.exe, 00000000.00000003.26840014 1.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comyle	JULY SOA.exe, 00000000.00000003.26473400 9.0000000005A7D000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000003.264473152.0000000005A7D000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000000.00000003.264579666.000000 0005A7D000.00000004.00000800.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadisglobal.com/cps0	JULY SOA.exe, 00000010.00000003.38838615 8.0000000006C41000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	JULY SOA.exe, 00000010.00000002.56250578 3.00000000060F1000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000002.551057155.0000000002D9E000. 00000004.00000800.00020000.00000000.sdmp, DnDcR.exe, 0000001B.00000002.551678919 .000000000341A000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	JULY SOA.exe, 00000010.00000002.56250578 3.00000000060F1000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000002.551057155.0000000002D9E000. 00000004.00000800.00020000.00000000.sdmp, DnDcR.exe, 0000001B.00000002.551678919 .000000000341A000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	DnDcR.exe, 0000001B.00000002.536397827.0 0000000030C1000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	JULY SOA.exe, 00000000.00000003.25993133 4.0000000005A94000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000002.336085792.0000000006CF2000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000000.00000003.259902767.000000 0005A93000.00000004.00000800.00020000.00 000000.sdmp	false		high
http://www.sandoll.co.kr	JULY SOA.exe, 00000000.00000002.33608579 2.0000000006CF2000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000003.261364106.0000000005A79000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	JULY SOA.exe, 00000000.00000003.26840014 1.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	JULY SOA.exe, 00000010.00000003.38853275 5.000000000611C000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.389668840.0000000006159000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comx	JULY SOA.exe, 00000000.00000003.25990276 7.0000000005A93000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/AC/RC/ocsp0c	JULY SOA.exe, 00000010.00000002.56310974 4.0000000006121000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comsiva	JULY SOA.exe, 00000000.00000003.26840014 1.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnLog	JULY SOA.exe, 00000000.00000003.26228740 9.0000000005A74000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.oaticerts.com/repository.	JULY SOA.exe, 00000010.00000003.38853275.000000000611C000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.0000000006159000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	JULY SOA.exe, 00000010.00000003.388386158.0000000006C41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comTTFq	JULY SOA.exe, 00000000.00000003.268400141.0000000005A79000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%appdata	JULY SOA.exe, 00000010.00000002.535440551.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, DnDcR.exe, 0000001B.00000002.536397827.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://ocsp.accv.es0	JULY SOA.exe, 00000010.00000003.390489017.000000000613A000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cni:	JULY SOA.exe, 00000000.00000003.262198978.0000000005AAD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	JULY SOA.exe, 00000010.00000003.390747397.0000000006122000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.echoworx.com/ca/root2/cps.pdf0	JULY SOA.exe, 00000010.00000003.390747397.0000000006122000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.389668840.0000000006159000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	JULY SOA.exe, 00000010.00000003.390243547.0000000006149000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-std0	JULY SOA.exe, 00000010.00000003.387953820.0000000006178000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.390747397.0000000006122000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388386158.0000000006C41000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	JULY SOA.exe, 00000010.00000003.390243547.0000000006149000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.388532755.000000000611C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	JULY SOA.exe, 00000000.00000002.336085792.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	JULY SOA.exe, 00000000.00000003.262287409.0000000005A74000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000000.00000002.336085792.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	JULY SOA.exe, 00000010.00000002.563299618.000000000617E000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.387953820.0000000006178000.00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000010.00000003.390115378.000000000617E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	JULY SOA.exe, 00000000.00000003.267569141.0000000005AAD000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.	JULY SOA.exe, 00000000.00000003.26840014 1.0000000005A79000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000003.267502782.0000000005A7A000. 00000004.00000800.00020000.00000000.sdmp, JULY SOA.exe, 00000000.00000003.267065355.000000 0005A79000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.defence.gov.au/pki0	JULY SOA.exe, 00000010.00000003.39074739 7.0000000006122000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel05	JULY SOA.exe, 00000010.00000003.38795382 0.0000000006178000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdsed	JULY SOA.exe, 00000000.00000003.26750278 2.0000000005A7A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 000.00000003.267065355.0000000005A79000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.gva.es/cps0%	JULY SOA.exe, 00000010.00000003.39048901 7.000000000613A000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.cert.fnmt.es/dpcs/0	JULY SOA.exe, 00000010.00000003.39074739 7.0000000006122000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-bt0	JULY SOA.exe, 00000010.00000002.53233598 8.0000000000E8C000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cnu-e	JULY SOA.exe, 00000000.00000003.26219897 8.0000000005AAD000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.comsign.co.il/cps0	JULY SOA.exe, 00000010.00000003.39024354 7.0000000006149000.00000004.00000800.000 20000.00000000.sdmp, JULY SOA.exe, 00000 010.00000003.388532755.000000000611C000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	JULY SOA.exe, 00000010.00000002.53544055 1.0000000002A41000.00000004.00000800.000 20000.00000000.sdmp, DnDcR.exe, 0000001B .00000002.536397827.00000000030C1000.000 00004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.e-me.lv/repository0	JULY SOA.exe, 00000010.00000003.38774872 2.0000000006C4F000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.136.29.110	palumalimited.com	United States		33494	IHNETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680518
Start date and time: 08/08/202218:19:05	2022-08-08 18:19:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JULY SOA.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@19/10@4/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 173.222.108.210, 173.222.108.226, 178.79.225.128, 95.140.230.192, 40.125.122.176, 20.54.89.106, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:20:27	API Interceptor	571x Sleep call for process: JULY SOA.exe modified
18:20:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run DnDcR C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
18:20:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run DnDcR C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
18:21:22	API Interceptor	150x Sleep call for process: DnDcR.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C..... .`h!0.I.(C..1Q*L.p.."s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x..... ...\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`. .u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i ....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

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

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	data
Category:	modified
Size (bytes):	290
Entropy (8bit):	2.934941215103815
Encrypted:	false
SSDEEP:	3:kkFklEBPtfllXlE/6hpllGhlR6pFRltB+SliQlP8F+RlTRe86A+iRlERMta9b3+O:kKE+N+SkQlPlEGYRMY9z+4KlDA3RUe/
MD5:	719153A58838CD7A751A8F220607D108
SHA1:	4A69BECA63D809EE4220D1DD784CF902A5EBFF40
SHA-256:	2E1C5BA075B29F9FC4A3FD8DD3EA0E59456AF2B614C43AFDAEF48925B28ABE6A
SHA-512:	8ED806F0558FF6CF3135AE1189A21BCE52BF7226A9C420831F5FD4F800C764336A52E7BCACED9ABD83D420FCB4D162F14CC56F49ED2B9DB45DC357642745E97
Malicious:	false
Reputation:	low
Preview:	p..... .....u.....(..... .....L.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DnDcR.exe.log

Process:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JULY SOA.exe.log

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp158E.tmp

Process:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191960058252804
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBdtn:cbh47TlNQ//rydbz9I3YODOLNdq3N
MD5:	2DE66077C08D213284FB641F42335869
SHA1:	426563B3B48D9533906C35B70F5CE005AF6BC6CB
SHA-256:	362F33AD691EC088848B51FE8057FDE1D6DB513927C110845ED007973F7D048A
SHA-512:	433FC5057017E06EC517377178C27A2D0279A98496ADF4A41EFE992B037A16CEAF3EB303EC6849D64BFC8187D9D1D55D23AA2CD104C91511121D20BBB0E5E42 2
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191960058252804
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBdtn:cbh47TlNQ//rydbz9I3YODOLNdq3N
MD5:	2DE66077C08D213284FB641F42335869
SHA1:	426563B3B48D9533906C35B70F5CE005AF6BC6CB
SHA-256:	362F33AD691EC088848B51FE8057FDE1D6DB513927C110845ED007973F7D048A
SHA-512:	433FC5057017E06EC517377178C27A2D0279A98496ADF4A41EFE992B037A16CEAF3EB303EC6849D64BFC8187D9D1D55D23AA2CD104C91511121D20BBB0E5E42 2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	889344
Entropy (8bit):	7.417227413730486
Encrypted:	false
SSDEEP:	24576:QEsjwi9BHtgLY40Sz1Zwfqh894DUM5fo:yRBN8Y40Sz36BK
MD5:	C059FD1E2EC2DF2B8E4AF62359868B1B
SHA1:	5CFADF7C20971459DADEAE535E61BCC6B6175DF0
SHA-256:	6C9947DD57C1A90267929341FFB0A7FF7F2251567481608 52A78DD83D6943578
SHA-512:	55B08020B882BFFA2E564098FE0EFFD718CD6FB63B89A2BE884BDC392C08BE89459F7ADD20BDFD7DE1A65A99CFB7D5A84ABA08CA4355DE94EA863AF939F45BA3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P..\|..... .....@.. ....@.....K..... ....H.....text....{.. ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....0.....*....0.....(!...*..0..:.....("... ... /...a%..^E.....+... @@B.Z .J_.a+.*...0..3..... s#.....s$.....s%.....s&.....s'.....*..0..?..... .... [:].a%..^E.....+.~....o(..... %..%Z .+p.a+..*..0..R..... ".C. M...a%..^E.....+.....+)~....o)..... k.4.Z ....a+.. .2..Z DL..a+..*...0..R..... u.a} ..e.a%..^E.....+.....+)~....o*.....

C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\qOHVWexsnI.exe

Process:	C:\Users\user\Desktop\JULY SOA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	889344
Entropy (8bit):	7.417227413730486
Encrypted:	false
SSDEEP:	24576:QEsjwi9BHtgLY40Sz1Zwfqh894DUM5fo:yRBN8Y40Sz36BK
MD5:	C059FD1E2EC2DF2B8E4AF62359868B1B
SHA1:	5CFADF7C20971459DADEAE535E61BCC6B6175DF0
SHA-256:	6C9947DD57C1A90267929341FFB0A7FF7F2251567481608 52A78DD83D6943578
SHA-512:	55B08020B882BFFA2E564098FE0EFFD718CD6FB63B89A2BE884BDC392C08BE89459F7ADD20BDFD7DE1A65A99CFB7D5A84ABA08CA4355DE94EA863AF939F45BA3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P..\|..... .....@.. ....@.....K..... ....H.....text....{.. ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....0.....*....0.....(!...*..0..:.....("... ... /...a%..^E.....+... @@B.Z .J_.a+.*...0..3..... s#.....s$.....s%.....s&.....s'.....*..0..?..... .... [:].a%..^E.....+.~....o(..... %..%Z .+p.a+..*..0..R..... ".C. M...a%..^E.....+.....+)~....o)..... k.4.Z ....a+.. .2..Z DL..a+..*...0..R..... u.a} ..e.a%..^E.....+.....+)~....o*.....

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\JULY SOA.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.417227413730486
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	JULY SOA.exe
File size:	889344
MD5:	c059fd1e2ec2df2b8e4af62359868b1b
SHA1:	5cfadf7c20971459dadeae535e61bcc6b6175df0
SHA256:	6c9947dd57c1a90267929341ffb0a7ff7f225156748160852a78dd83d6943578
SHA512:	55b08020b882bffa2e564098fe0effd718cd6fb63b89a2be884bdc392c08be89459f7add20bdfd7de1a65a99cfb7d5a84aba08ca4355de94ea863af939f45ba3
SSDEEP:	24576:QEsjwi9BHtgLY40Sz1Zwfqh894DUM5fo:yRBN8Y40Sz36BK
TLSH:	5B155BA9319071DFD923CA31CAA41C74EB617C77A71B921794673298DB3E987DF200B2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P..|..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d9afe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F09691 [Mon Aug 8 04:52:33 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd9ab0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xda000	0x11f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdc000	0xc	.reloc
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd7b04	0xd7c00	False	0.7431821679461182	data	7.420583605513861	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xda000	0x11f0	0x1200	False	0.3936631944444444	data	5.051410354326853	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.041015625	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

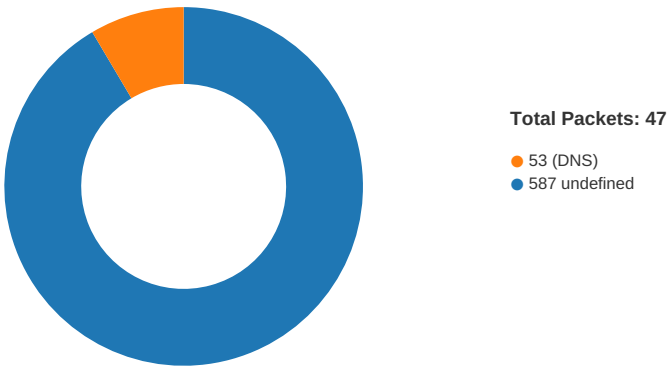
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xda0a0	0x334	data		
RT_MANIFEST	0xda3d4	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:21:04.948134899 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.083220005 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.083420038 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.273957968 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.274281025 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.411305904 CEST	587	49766	174.136.29.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:21:05.412811041 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.550263882 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.673643112 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.816494942 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.816524029 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.816540956 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.816554070 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.816620111 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.818304062 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.818408012 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:05.842231989 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:05.977404118 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:06.087069988 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:15.787471056 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:15.922790051 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:15.924426079 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.059607029 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.060353994 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.199578047 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.200393915 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.335732937 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.336157084 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.510190964 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.510229111 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.510598898 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.645215988 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.645272970 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.646442890 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.646557093 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.647399902 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.647458076 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:21:16.781286955 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.781354904 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.781837940 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.781985044 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.790127039 CEST	587	49766	174.136.29.110	192.168.2.3
Aug 8, 2022 18:21:16.900490999 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:13.665323973 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:13.800867081 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:13.801105976 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:13.974426985 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:13.974801064 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.110100985 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.146116018 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.283982992 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.483633041 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.677851915 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.824517012 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.824542046 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.824558020 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.824564934 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.824764967 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.824806929 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:14.828706026 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:14.983639002 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:15.217648983 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:15.353404045 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:15.593067884 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:16.751756907 CEST	49783	587	192.168.2.3	174.136.29.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:22:16.887917042 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:16.888345957 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.024554014 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.024955034 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.164678097 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.165038109 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.300569057 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.300832987 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.476304054 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.479221106 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.479465008 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.617343903 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.617388010 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.618134975 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.618186951 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.618196011 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.618211031 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:17.754057884 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.754098892 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.754127979 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.754143953 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.770174026 CEST	587	49783	174.136.29.110	192.168.2.3
Aug 8, 2022 18:22:17.967497110 CEST	49783	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:41.594635010 CEST	49766	587	192.168.2.3	174.136.29.110
Aug 8, 2022 18:22:41.769206047 CEST	587	49766	174.136.29.110	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:21:03.302783012 CEST	49327	53	192.168.2.3	8.8.8.8
Aug 8, 2022 18:21:03.595026016 CEST	53	49327	8.8.8.8	192.168.2.3
Aug 8, 2022 18:21:04.810533047 CEST	51391	53	192.168.2.3	8.8.8.8
Aug 8, 2022 18:21:04.827919960 CEST	53	51391	8.8.8.8	192.168.2.3
Aug 8, 2022 18:22:13.003118992 CEST	59795	53	192.168.2.3	8.8.8.8
Aug 8, 2022 18:22:13.284246922 CEST	53	59795	8.8.8.8	192.168.2.3
Aug 8, 2022 18:22:13.325135946 CEST	59390	53	192.168.2.3	8.8.8.8
Aug 8, 2022 18:22:13.617414951 CEST	53	59390	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 18:21:03.302783012 CEST	192.168.2.3	8.8.8.8	0xaf9a	Standard query (0)	mail.palumalimited.com	A (IP address)	IN (0x0001)
Aug 8, 2022 18:21:04.810533047 CEST	192.168.2.3	8.8.8.8	0x4ab1	Standard query (0)	mail.palumalimited.com	A (IP address)	IN (0x0001)
Aug 8, 2022 18:22:13.003118992 CEST	192.168.2.3	8.8.8.8	0xb412	Standard query (0)	mail.palumalimited.com	A (IP address)	IN (0x0001)
Aug 8, 2022 18:22:13.325135946 CEST	192.168.2.3	8.8.8.8	0xd476	Standard query (0)	mail.palumalimited.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 18:21:03.595026016 CEST	8.8.8.8	192.168.2.3	0xaf9a	No error (0)	mail.palumalimited.com	palumalimited.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:21:03.595026016 CEST	8.8.8.8	192.168.2.3	0xaf9a	No error (0)	palumalimited.com		174.136.29.110	A (IP address)	IN (0x0001)
Aug 8, 2022 18:21:04.827919960 CEST	8.8.8.8	192.168.2.3	0x4ab1	No error (0)	mail.palumalimited.com	palumalimited.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:21:04.827919960 CEST	8.8.8.8	192.168.2.3	0x4ab1	No error (0)	palumalimited.com		174.136.29.110	A (IP address)	IN (0x0001)

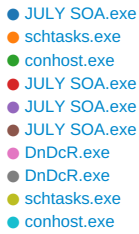
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 18:21:09.125080109 CEST	8.8.8.8	192.168.2.3	0x7fa2	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.128	A (IP address)	IN (0x0001)
Aug 8, 2022 18:21:09.125080109 CEST	8.8.8.8	192.168.2.3	0x7fa2	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)
Aug 8, 2022 18:21:13.981113911 CEST	8.8.8.8	192.168.2.3	0xebaa	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)
Aug 8, 2022 18:21:13.981113911 CEST	8.8.8.8	192.168.2.3	0xebaa	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)
Aug 8, 2022 18:22:13.284246922 CEST	8.8.8.8	192.168.2.3	0xb412	No error (0)	mail.palumalimited.com	palumalimited.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:22:13.284246922 CEST	8.8.8.8	192.168.2.3	0xb412	No error (0)	palumalimited.com		174.136.29.110	A (IP address)	IN (0x0001)
Aug 8, 2022 18:22:13.617414951 CEST	8.8.8.8	192.168.2.3	0xd476	No error (0)	mail.palumalimited.com	palumalimited.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:22:13.617414951 CEST	8.8.8.8	192.168.2.3	0xd476	No error (0)	palumalimited.com		174.136.29.110	A (IP address)	IN (0x0001)

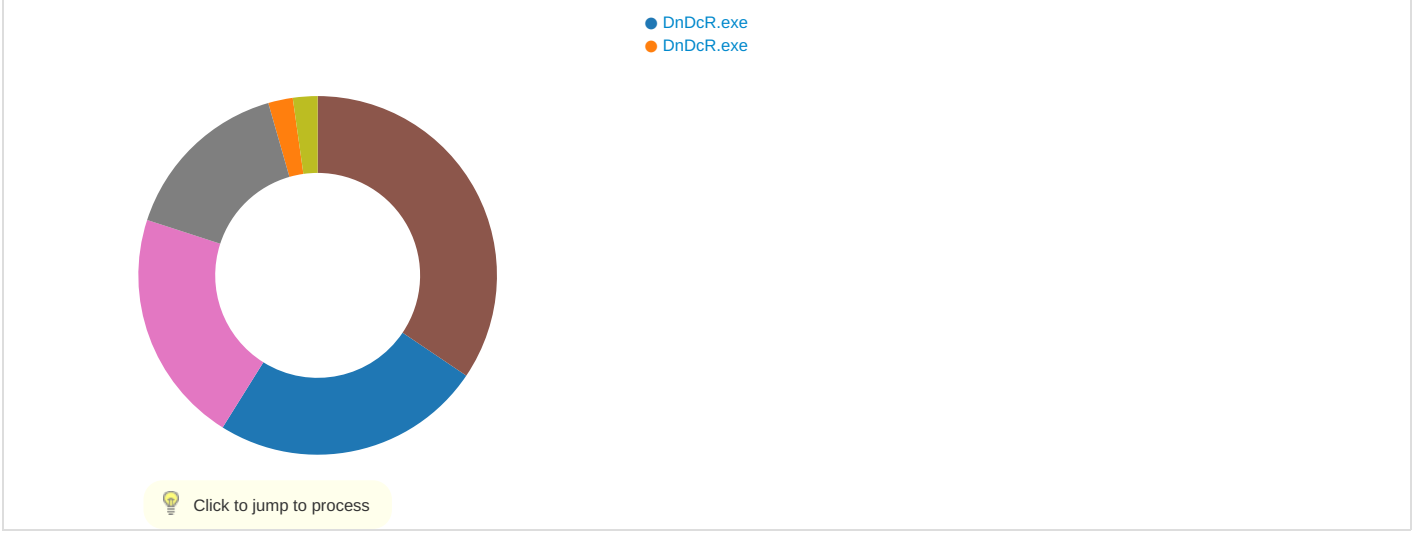
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 18:21:05.273957968 CEST	587	49766	174.136.29.110	192.168.2.3	220-fastest.vivawebhost.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 12:21:05 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 18:21:05.274281025 CEST	49766	587	192.168.2.3	174.136.29.110	EHLO 472847
Aug 8, 2022 18:21:05.411305904 CEST	587	49766	174.136.29.110	192.168.2.3	250-fastest.vivawebhost.com Hello 472847 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 18:21:05.412811041 CEST	49766	587	192.168.2.3	174.136.29.110	STARTTLS
Aug 8, 2022 18:21:05.550263882 CEST	587	49766	174.136.29.110	192.168.2.3	220 TLS go ahead
Aug 8, 2022 18:22:13.974426985 CEST	587	49783	174.136.29.110	192.168.2.3	220-fastest.vivawebhost.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 12:22:14 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 18:22:13.974801064 CEST	49783	587	192.168.2.3	174.136.29.110	EHLO 472847
Aug 8, 2022 18:22:14.110100985 CEST	587	49783	174.136.29.110	192.168.2.3	250-fastest.vivawebhost.com Hello 472847 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 18:22:14.146116018 CEST	49783	587	192.168.2.3	174.136.29.110	STARTTLS
Aug 8, 2022 18:22:14.283982992 CEST	587	49783	174.136.29.110	192.168.2.3	220 TLS go ahead

Statistics

Behavior





System Behavior

Analysis Process: JULY SOA.exe PID: **5808**, Parent PID: **5284**

General

Target ID:	0
Start time:	18:20:10
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\JULY SOA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\JULY SOA.exe"
Imagebase:	0x680000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.319820199.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	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	6CDECF06	unknown
C:\Users\user\AppData\Roaming\qOHVWexsnI.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BC31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC37038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JULY SOA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D0FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp	success or wait	1	6BC36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\qOHVWexsnI.exe	0	889344	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 7c 0d 00 00 14 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 fd 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELbP| @ @	success or wait	1	6BC31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp	0	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	6BC31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JULY SOA.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D0FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Users\user\Desktop\JULY SOA.exe	unknown	889344	success or wait	1	6BC31B4F	ReadFile

Analysis Process: schtasks.exe PID: **2232**, Parent PID: **5808**

General

Target ID:	8
Start time:	18:20:32
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qOHVWexsnI" /XML "C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp
Imagebase:	0xa90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

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\AppData\Local\Temp\tmp3EB6.tmp	unknown	2	success or wait	1	A9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3EB6.tmp	unknown	1644	success or wait	1	A9ABD9	ReadFile

Analysis Process: conhost.exe PID: **2292**, Parent PID: **2232**

General

Target ID:	10
Start time:	18:20:33
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: JULY SOA.exe PID: **5668**, Parent PID: **5808**

General

Target ID:	12
Start time:	18:20:34
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\JULY SOA.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x80000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: JULY SOA.exe PID: **4588**, Parent PID: **5808**

General

Target ID:	15
Start time:	18:20:35
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\JULY SOA.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x30000
File size:	889344 bytes

MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: JULY SOA.exe PID: **4972**, Parent PID: **5808**

General

Target ID:	16
Start time:	18:20:36
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\JULY SOA.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6b0000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.535440551.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.535440551.0000000002A41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.308754595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.308754595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000010.00000000.308754595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	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	6CDECF06	unknown
C:\Users\user\AppData\Roaming\DnDcR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BC3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BC3DD66	CopyFileW
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BC3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe:Zone.Identifier	success or wait	1	6CC5EAF6	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BC31B4F	WriteFile
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 7c 0d 00 00 14 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 fd 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELbP| @ @	success or wait	4	6BC3DD66	CopyFileW
C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6BC3DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d85e7350-a0ca-4f4d-bb14-cc08b64aaacc	unknown	4096	success or wait	1	6BC31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC31B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	DnDcR	unicode	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe	success or wait	1	6BC3646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	DnDcR	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BC3DE2E	RegSetValueExW

Analysis Process: DnDcR.exe PID: **2080**, Parent PID: **3968**

General

Target ID:	19
Start time:	18:20:52
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe"
Imagebase:	0xea0000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.450194726.0000000004362000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.450194726.0000000004362000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000013.00000002.450194726.0000000004362000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	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	6CDECF06	unknown
C:\Users\user\AppData\Local\Temp\tmp158E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BC37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DnDcR.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D0FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp158E.tmp	success or wait	1	6BC36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp158E.tmp	0	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6BC31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DnDcR.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D0FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile

Analysis Process: DnDcR.exe PID: **3168**, Parent PID: **3968**

General

Target ID:	21
Start time:	18:21:01
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe"
Imagebase:	0xab0000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDECF06	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	6CDECF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC31B4F	ReadFile

Analysis Process: schtasks.exe PID: **5508**, Parent PID: **2080**

General

Target ID:	24
Start time:	18:21:28
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qOHVWexsnI" /XML "C:\Users\user\AppData\Local\Temp\tmp158E.tmp
Imagebase:	0xa90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

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\AppData\Local\Temp\tmp158E.tmp	unknown	2	success or wait	1	A9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp158E.tmp	unknown	1644	success or wait	1	A9ABD9	ReadFile

Analysis Process: conhost.exe PID: **5496**, Parent PID: **5508**

General

Target ID:	25
Start time:	18:21:29
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: DnDcR.exe PID: **5900**, Parent PID: **2080**

General

Target ID:	26
Start time:	18:21:30
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x70000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DnDcR.exe PID: **3896**, Parent PID: **2080**

General	
Target ID:	27
Start time:	18:21:31
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\DnDcR\DnDcR.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbc0000
File size:	889344 bytes
MD5 hash:	C059FD1E2EC2DF2B8E4AF62359868B1B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000002.536397827.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001B.00000002.536397827.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly