

ID: 715065
Sample Name:
QNx8Bu7CNn.exe
Cookbook: default.jbs
Time: 15:48:08
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report QNx8Bu7CNn.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 11
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNx8Bu7CNn.exe.log 13
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 14
Entrypoint Preview 14
Data Directories 16
Sections 16
Resources 16
Imports 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
FTP Packets 17
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: QNx8Bu7CNn.exePID: 5292, Parent PID: 3320 18

General 18
File Activities 19
File Created 19
File Written 19
File Read 19
Analysis Process: QNx8Bu7CNn.exePID: 5840, Parent PID: 5292 20
General 20
File Activities 20
File Created 20
File Read 20
Registry Activities 21
Disassembly 21

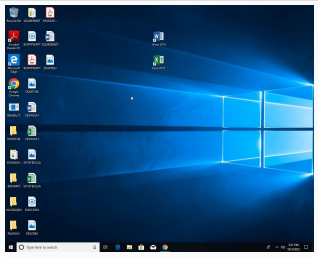
Windows Analysis Report

QNx8Bu7CNn.exe

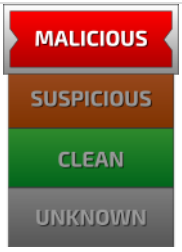
Overview

General Information

Sample Name:	QNx8Bu7CNn.exe
Analysis ID:	715065
MD5:	9a9cb1f7f37aa39..
SHA1:	8d63b02db5ce9b..
SHA256:	943089ba13faf44..
Tags:	AgentTesla exe
Infos:	



Detection



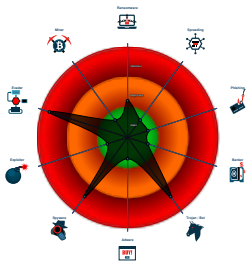
AgentTesla

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
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- QNx8Bu7CNn.exe (PID: 5292 cmdline: C:\Users\user\Desktop\QNx8Bu7CNn.exe MD5: 9A9CB1F7F37AA3955CFB4D8991583E31)
  - QNx8Bu7CNn.exe (PID: 5840 cmdline: C:\Users\user\Desktop\QNx8Bu7CNn.exe MD5: 9A9CB1F7F37AA3955CFB4D8991583E31)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "FTP",
  "FTP Host": "ftp://ftp.valvulasthermovalve.cl/",
  "Username": "cva19491@valvulasthermovalve.cl",
  "Password": "LILKOOLL14!!"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30080:$a13: get_DnsResolver • 0x2e88e:$a20: get_LastAccessed • 0x309fe:$a27: set_InternalServerPort • 0x30d1a:$a30: set_GuidMasterKey • 0x2e995:$a33: get_Clipboard • 0x2e9a3:$a34: get_Keyboard • 0x2fcb3:$a35: get_ShiftKeyDown • 0x2fcc4:$a36: get_AltKeyDown • 0x2e9b0:$a37: get_Password • 0x2f463:$a38: get_PasswordHash • 0x30480:$a39: get_DefaultCredentials
00000000.00000002.278449042.000000000477F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.278449042.000000000477F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.QNx8Bu7CNn.exe.47e9d28.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.QNx8Bu7CNn.exe.47e9d28.8.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.QNx8Bu7CNn.exe.47e9d28.8.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b4d:$s10: logins • 0x66f6d:$s10: logins • 0x325b4:$s11: credential • 0x669d4:$s11: credential • 0x2eb95:$g1: get_Clipboard • 0x62fb5:$g1: get_Clipboard • 0x2eba3:$g2: get_Keyboard • 0x62fc3:$g2: get_Keyboard • 0x2ebb0:$g3: get_Password • 0x62fd0:$g3: get_Password • 0x2fea3:$g4: get_CtrlKeyDown • 0x642c3:$g4: get_CtrlKeyDown • 0x2feb3:$g5: get_ShiftKeyDown • 0x642d3:$g5: get_ShiftKeyDown • 0x2fec4:$g6: get_AltKeyDown • 0x642e4:$g6: get_AltKeyDown
0.2.QNx8Bu7CNn.exe.47e9d28.8.raw.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30280:$a13: get_DnsResolver • 0x646a0:$a13: get_DnsResolver • 0x2ea8e:$a20: get_LastAccessed • 0x62eae:$a20: get_LastAccessed • 0x30bfe:$a27: set_InternalServerPort • 0x6501e:$a27: set_InternalServerPort • 0x30f1a:$a30: set_GuidMasterKey • 0x6533a:$a30: set_GuidMasterKey • 0x2eb95:$a33: get_Clipboard • 0x62fb5:$a33: get_Clipboard • 0x2eba3:$a34: get_Keyboard • 0x62fc3:$a34: get_Keyboard • 0x2feb3:$a35: get_ShiftKeyDown • 0x642d3:$a35: get_ShiftKeyDown • 0x2fec4:$a36: get_AltKeyDown • 0x642e4:$a36: get_AltKeyDown • 0x2ebb0:$a37: get_Password • 0x62fd0:$a37: get_Password • 0x2f663:$a38: get_PasswordHash • 0x63a83:$a38: get_PasswordHash • 0x30680:$a39: get_DefaultCredentials
0.2.QNx8Bu7CNn.exe.47e9d28.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



.NET source code contains potential unpacker

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



Injects a PE file into a foreign processes

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



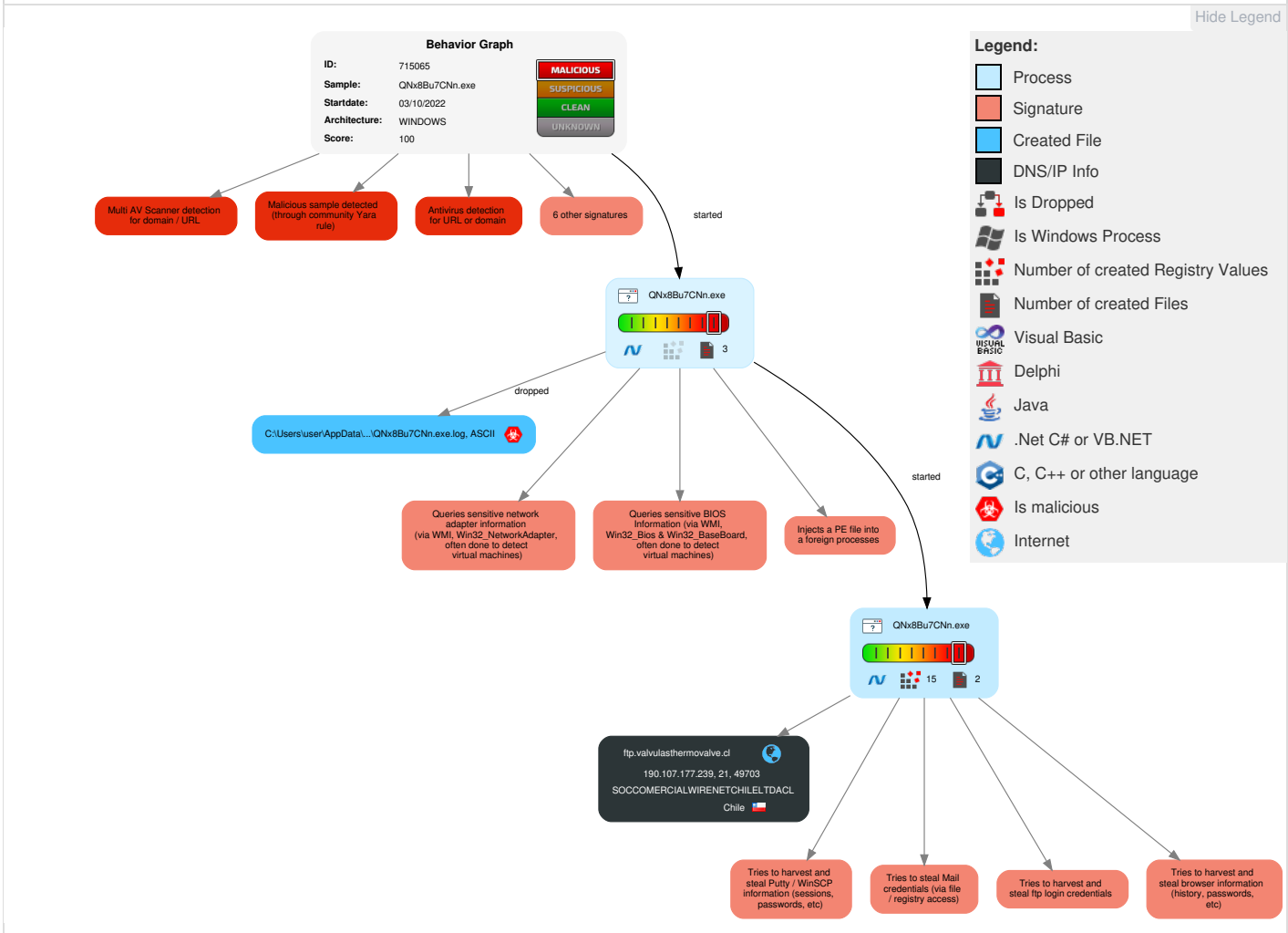
Yara detected AgentTesla

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	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	1 Exfiltration Over Alternative Protocol	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	1 1 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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System 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 1 Software Packing	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

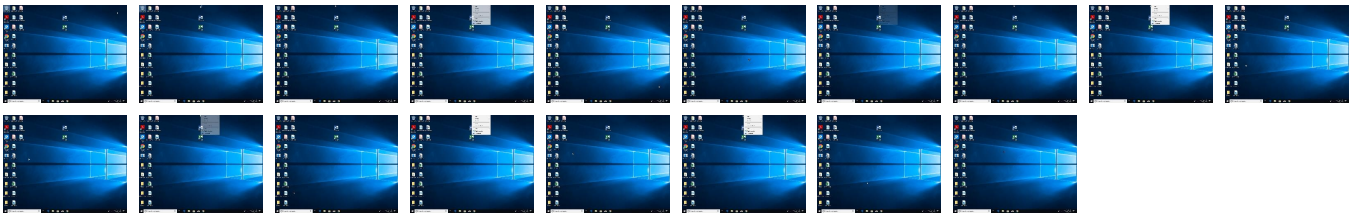
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QNx8Bu7CNn.exe	27%	ReversingLabs		
QNx8Bu7CNn.exe	32%	Virustotal		Browse
QNx8Bu7CNn.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.QNx8Bu7CNn.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
ftp.valvulasthermovalve.cl	17%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://pzxuZU.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ftp://ftp.valvulasthermovalve.cl/cva19491	100%	URL Reputation	phishing	
http://uZTc8nGgAr9KT9EFaKnD.net	0%	Avira URL Cloud	safe	
http://ftp.valvulasthermovalve.cl	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.valvulasthermovalve.cl	190.107.177.239	true	false	• 17%, Virustotal, Browse	unknown

URLs from Memory and Binaries

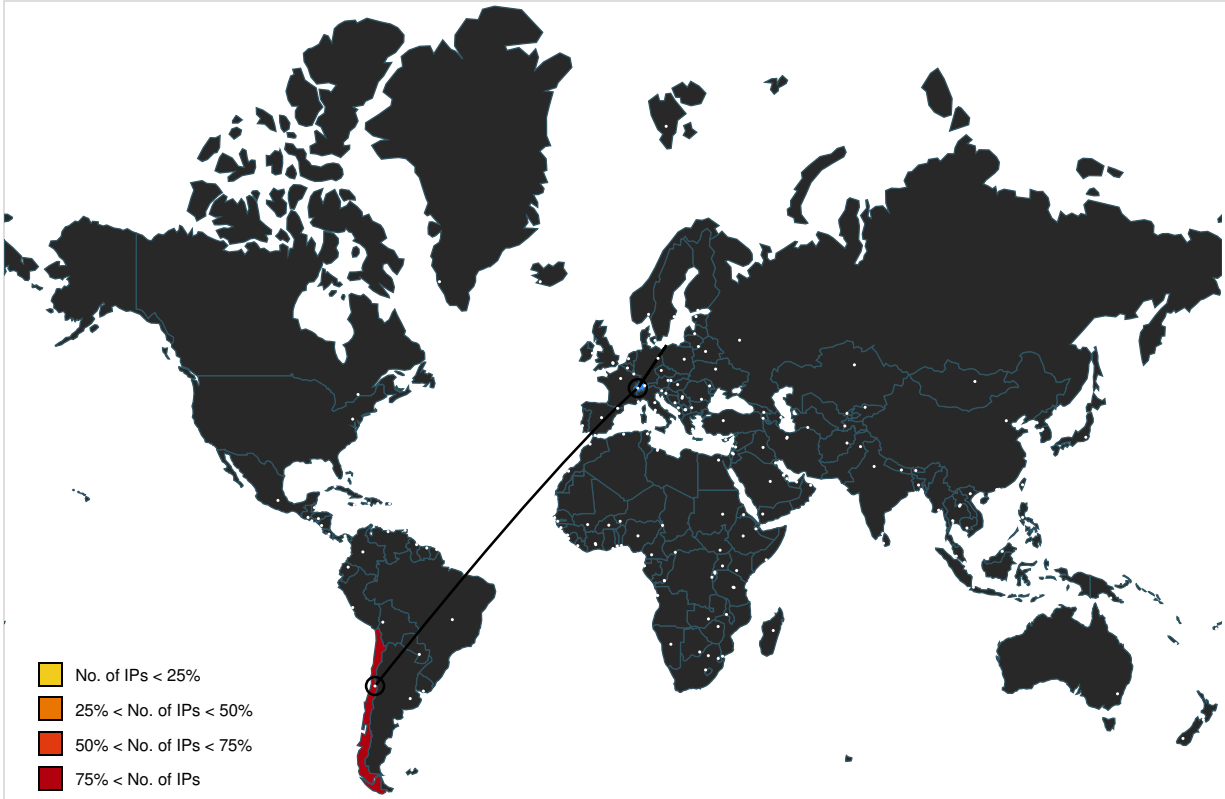
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high

Copyright Joe Security LLC 2022

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ftp.valvulasthermovalve.cl	QNx8Bu7CNn.exe, 00000001.00000002.510640859.0000000002C75000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.fontbureau.com/designers/?	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://uZTc8nGgAr9KT9EFaKnD.net	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp, QNx8Bu7CNn.exe, 00000001.00000002.510594948.0000000002C69000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pzxuZU.com	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	QNx8Bu7CNn.exe, 00000001.00000002.510594948.0000000002C69000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	QNx8Bu7CNn.exe, 00000000.00000002.280625866.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ftp://ftp.valvulasthermovalve.cl/cva19491	QNx8Bu7CNn.exe, 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp	true	• URL Reputation: phishing	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.107.177.239	ftp.valvulasthermovalve.cl	Chile		265831	SOCCOMERCIALWIRENETCHILELTDACL	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715065
Start date and time:	2022-10-03 15:48:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2022

Report type:	light
Sample file name:	QNx8Bu7CNn.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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.spyw.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 8.238.190.126, 8.238.85.254, 8.248.131.254, 67.26.139.254, 8.253.207.120, 93.184.221.240
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.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 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
15:49:11	API Interceptor	723x Sleep call for process: QNx8Bu7CNn.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\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNx8Bu7CNn.exe.log

Process:	C:\Users\user\Desktop\QNx8Bu7CNn.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.560020608920164
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:	QNx8Bu7CNn.exe
File size:	909824
MD5:	9a9cb1f7f37aa3955cfb4d8991583e31
SHA1:	8d63b02db5ce9bb9bb1691ab4a5282d18078191a
SHA256:	943089ba13faf44a75c9624e2b68af1f561d5567bb4ba7cf4a2596b129da6a2b
SHA512:	d018ecbd1cb1cea36a4e24e30525e64a1e44d0505859de1dcb93511d2e5a77f508ed0284114387da67dfcb0294d5bd15e5cf9d8629adc99e013660affa2dbac4
SSDEEP:	12288:kK4HTNWk67oi/z0xXi5nv9OZT5fEKD501+owI73IskA2IaBunfuEhp+0:ME4xgv9OjbD/owE3IsH2cnmS
TLSH:	2F15D02107E19B0BC0525374CDD2C3B0AFE84EB5E6B5C2874FE9FD9BB5771AAAA00145
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f.:c.....0..... .....@.. .....@.....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4df4c2
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:	0x633AA966 [Mon Oct 3 09:20:38 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

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

Instruction
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	0xdf470	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x608	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	
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	0xdd4c8	0xdd600	False	0.6838815905561829	data	6.567722609504779	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x608	0x800	False	0.3310546875	data	3.444132612113464	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0090	0x378	data		
RT_MANIFEST	0xe0418	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

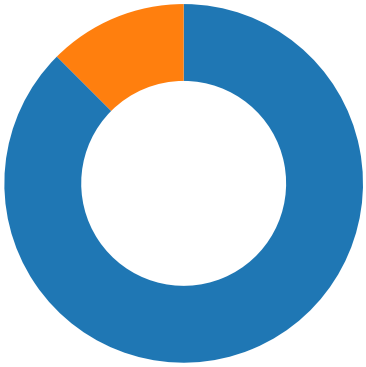
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 8

- 53 (DNS)
- 21 (FTP -- Control)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:49:31.703001976 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:31.954325914 CEST	21	49703	190.107.177.239	192.168.2.7
Oct 3, 2022 15:49:31.954523087 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:31.960650921 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:32.201725006 CEST	21	49703	190.107.177.239	192.168.2.7
Oct 3, 2022 15:49:32.201850891 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:32.207669973 CEST	21	49703	190.107.177.239	192.168.2.7
Oct 3, 2022 15:49:32.207695961 CEST	21	49703	190.107.177.239	192.168.2.7
Oct 3, 2022 15:49:32.207709074 CEST	21	49703	190.107.177.239	192.168.2.7
Oct 3, 2022 15:49:32.207739115 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:32.207787037 CEST	49703	21	192.168.2.7	190.107.177.239
Oct 3, 2022 15:49:32.207787037 CEST	49703	21	192.168.2.7	190.107.177.239

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:49:31.417812109 CEST	55752	53	192.168.2.7	8.8.8.8
Oct 3, 2022 15:49:31.685353041 CEST	53	55752	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:49:31.417812109 CEST	192.168.2.7	8.8.8.8	0xa279	Standard query (0)	ftp.valvul asthermovalve.cl	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 15:49:31.685353041 CEST	8.8.8.8	192.168.2.7	0xa279	No error (0)	ftp.valvul asthermova lve.cl		190.107.177.239	A (IP address)	IN (0x0001)	false

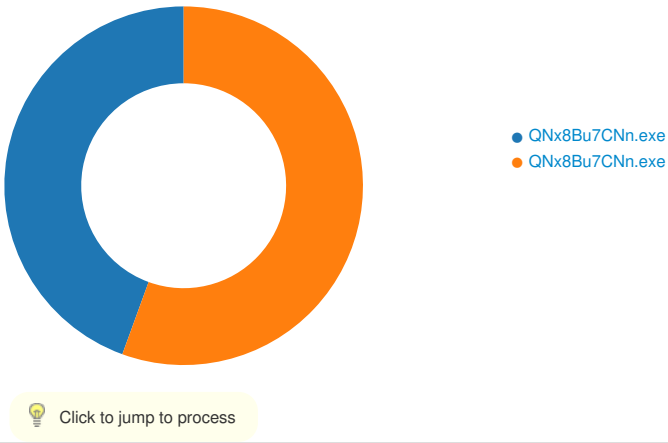
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 3, 2022 15:49:32.201725006 CEST	21	49703	190.107.177.239	192.168.2.7	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 10 of 100 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 10 of 100 allowed.220-Local time is now 09:49. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 10 of 100 allowed.220-Local time is now 09:49. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 10 of 100 allowed.220-Local time is now 09:49. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 10 of 100 allowed.220-Local time is now 09:49. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Oct 3, 2022 15:49:32.207695961 CEST	21	49703	190.107.177.239	192.168.2.7	220 Logout.

Statistics

Behavior



System Behavior

Analysis Process: QNx8Bu7CNn.exe PID: **5292**, Parent PID: **3320**

General

Target ID:	0
Start time:	15:49:01
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\QNx8Bu7CNn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QNx8Bu7CNn.exe
Imagebase:	0xf00000
File size:	909824 bytes
MD5 hash:	9A9CB1F7F37AA3955CFB4D8991583E31
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.278449042.000000000477F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.278449042.000000000477F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.278449042.000000000477F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.266177518.0000000003426000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5FCF06	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	6D5FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNx8Bu7CNn.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D90C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNx8Bu7CNn.exe.log	0	1308	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	6D90C907	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	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5303DE	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C441B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C441B4F	ReadFile

Analysis Process: QNx8Bu7CNn.exe PID: **5840**, Parent PID: **5292**

General

Target ID:	1
Start time:	15:49:13
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\QNx8Bu7CNn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QNx8Bu7CNn.exe
Imagebase:	0x500000
File size:	909824 bytes
MD5 hash:	9A9CB1F7F37AA3955CFB4D8991583E31
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: 00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.262156014.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.507516330.0000000002921000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5FCF06	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	6D5FCF06	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	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C441B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C441B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C441B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C441B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C441B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C441B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3d3bfcea-a92d-4141-afde-fa1cf8edbed3	unknown	4096	success or wait	1	6C441B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C441B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly