ID: 330378
Sample Name:
QNSpfBSrsR.exe
Cookbook: default.jbs
Time: 20:44:48
Date: 14/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report QNSpfBSrsR.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: HawkEye 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 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
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Authenticode Signature 13
Entrypoint Preview 14
Data Directories 15
Sections 15
Imports 16

Network Behavior 16
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: QNSpfBSrsR.exe PID: 6696 Parent PID: 5928 16
General 16
File Activities 17
File Created 17
File Written 17
File Read 17
Analysis Process: QNSpfBSrsR.exe PID: 7128 Parent PID: 6696 18
General 18
Analysis Process: QNSpfBSrsR.exe PID: 6384 Parent PID: 6696 18
General 18
Analysis Process: QNSpfBSrsR.exe PID: 2800 Parent PID: 6696 18
General 18
File Activities 19
File Created 19
File Deleted 20
File Written 20
File Read 20
Analysis Process: vbc.exe PID: 4204 Parent PID: 2800 20
General 20
Analysis Process: vbc.exe PID: 5732 Parent PID: 2800 21
General 21
Analysis Process: vbc.exe PID: 7132 Parent PID: 2800 21
General 21
Analysis Process: vbc.exe PID: 7012 Parent PID: 2800 22
General 22
Analysis Process: vbc.exe PID: 4088 Parent PID: 2800 22
General 22
Analysis Process: vbc.exe PID: 1072 Parent PID: 2800 22
General 22
Disassembly 23
Code Analysis 23

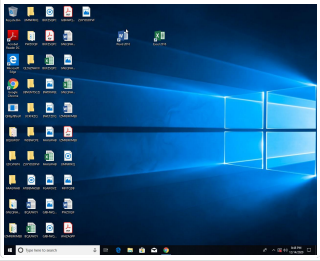
Analysis Report QNSpfBSrsR.exe

Overview

General Information

Sample Name:	QNSpfBSrsR.exe
Analysis ID:	330378
MD5:	7da4f5e17791a77.
SHA1:	552b4a357b2599..
SHA256:	ac8ef770d70da42.
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

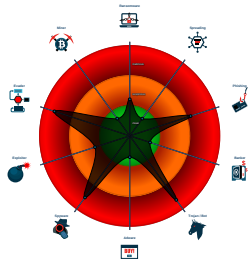
HawkEye M00nD3v Logger MailPassView

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

Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AntiVM_3
- Yara detected HawkEye Keylogger
- Yara detected M00nD3v Logger
- Yara detected MailPassView
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queries sensitive network adapter in…
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other

Classification



Startup

- **System is w10x64**
- QNSpfBSrsR.exe (PID: 6696 cmdline: 'C:\Users\user\Desktop\QNSpfBSrsR.exe' MD5: 7DA4F5E17791A774131C3C97538A2495)
  - QNSpfBSrsR.exe (PID: 7128 cmdline: C:\Users\user\Desktop\QNSpfBSrsR.exe MD5: 7DA4F5E17791A774131C3C97538A2495)
  - QNSpfBSrsR.exe (PID: 6384 cmdline: C:\Users\user\Desktop\QNSpfBSrsR.exe MD5: 7DA4F5E17791A774131C3C97538A2495)
  - QNSpfBSrsR.exe (PID: 2800 cmdline: C:\Users\user\Desktop\QNSpfBSrsR.exe MD5: 7DA4F5E17791A774131C3C97538A2495)
    - vbc.exe (PID: 4204 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9C49.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5732 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9C48.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 7132 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp989B.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 7012 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9CC3.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 4088 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp8FAF.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 1072 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9398.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "mailpv"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.739399669.000000000400000.00000040.00000001.sdmp	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
0000000B.00000002.739399669.000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000008.00000002.1020981161.000000000358C000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000014.00000002.1014010873.000000000400000.00000040.00000001.sdmp	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
00000014.00000002.1014010873.000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 32 entries				

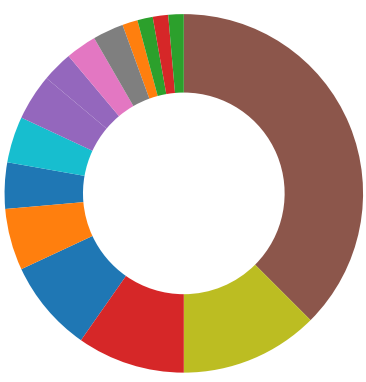
Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.vbc.exe.400000.0.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x131b0:$a1: logins.json • 0x13110:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x13934:$s4: \mozsqlite3.dll • 0x121a4:$s5: SMTP Password
11.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
10.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
10.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
8.2.QNSpfBSrsR.exe.3090000.2.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x134d2:$a1: logins.json • 0x13432:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x13c56:$s4: \mozsqlite3.dll • 0x124c6:$s5: SMTP Password
Click to see the 26 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger

System Summary:

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Sample uses process hollowing technique
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected HawkEye Keylogger
- Yara detected M00nD3v Logger
- Yara detected MailPassView
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Tries to steal Mail credentials (via file registry)

Remote Access Functionality:

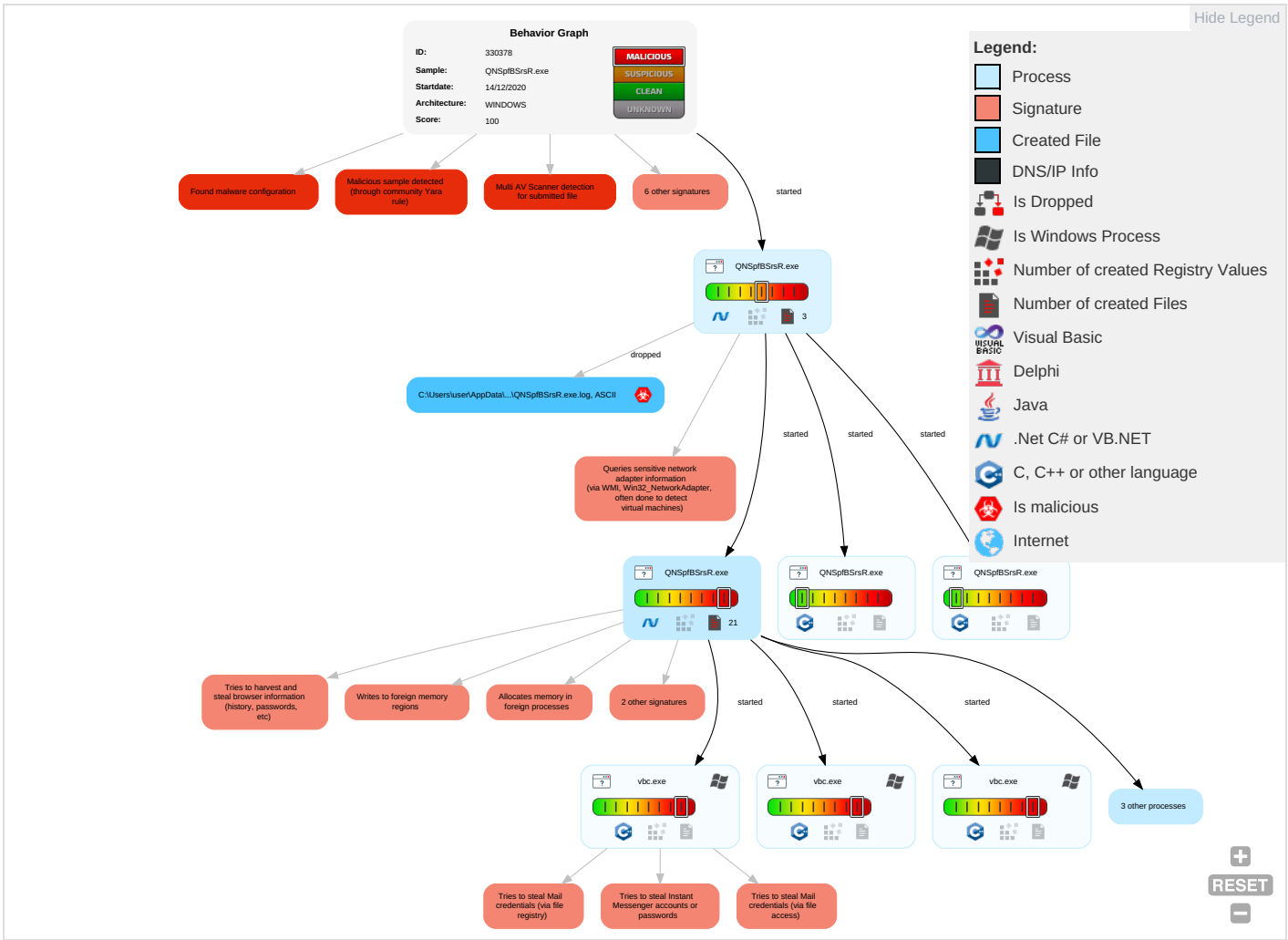
- Detected HawkEye Rat
- Yara detected HawkEye Keylogger
- Yara detected M00nD3v Logger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Remote Acces Software 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials In Files 1	System Information Discovery 1 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Security Software Discovery 2 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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
QNSpfBSrsR.exe	29%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.QNSpfBSrsR.exe.30000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
4.2.QNSpfBSrsR.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
4.0.QNSpfBSrsR.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.QNSpfBSrsR.exe.7f0000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
8.2.QNSpfBSrsR.exe.7f0000.1.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
8.2.QNSpfBSrsR.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.QNSpfBSrsR.exe.30000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
0.0.QNSpfBSrsR.exe.820000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll;HawkEye	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.phpCContent-Disposition:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=4510094	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://pomf.cat/upload.php&https://a.pomf.cat/	QNSpfBSrsR.exe, 00000008.00000002.1014445392.0000000000402000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://dyn.com/dns/	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false		high
http://pomf.cat/upload.php	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	QNSpfBSrsR.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1)	QNSpfBSrsR.exe, 00000008.00000003.736849493.0000000001556000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1LMEM	QNSpfBSrsR.exe, 00000008.00000003.736849493.0000000001556000.00000004.00000001.sdmp	false		high
http://bot.whatismyipaddress.com/	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false		high
http://www.msn.com/	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=8072167097284;g	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehp	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	QNSpfBSrsR.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.pomf.cat/	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1LMEM	QNSpfBSrsR.exe, 00000008.00000003.736849493.0000000001556000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	QNSpfBSrsR.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehp	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	QNSpfBSrsR.exe, 00000008.00000003.736849493.0000000001556000.00000004.00000001.sdmp, QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0D	QNSpfBSrsR.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/checksync.php	QNSpfBSrsR.exe, 00000008.00000002.1017856327.00000000032F7000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	vbc.exe, 00000014.00000002.1014010873.0000000000400000.00000040.00000001.sdmp	false		high
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll;HawkEye	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pomf.cat/upload.phpCContent-Disposition:	QNSpfBSrsR.exe, 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	330378
Start date:	14.12.2020
Start time:	20:44:48

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QNSpfBSrsR.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:	21
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.phis.troj.spyw.evad.winEXE@19/2@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.4% (good quality ratio 94.5%) • Quality average: 85.6% • Quality standard deviation: 23.2%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • 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
20:46:14	API Interceptor	4x Sleep call for process: QNSpfBSrsR.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNSpfBSrsR.exe.log	
Process:	C:\Users\user\Desktop\QNSpfBSrsR.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7K84j:MxHKX9HKnYHKhQnoPtHoxHhAHKzvKvj
MD5:	FC95B72FA9788BDF0B8075C768FFDCEB
SHA1:	2ED2BE675DAF980B3061A622CBF795050F9A68DC
SHA-256:	37D8549A8145090B163B3C5D4A91231AFE1F66E7C1A7203BDE5D48147B0C3B5E
SHA-512:	B6CDA7870B3154B1D77663E4005EFA1C4EA210F955456FC8F8B2445FFCD52B41EAFAC2144E4F1B3BC86D4604F0E86DF5664921C354B313EF7E256162D604E45
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Temp\2c99a7ed-ddac-ab7c-0bfe-56058ec17ef8	
Process:	C:\Users\user\Desktop\QNSpfBSrsR.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.170009133144317
Encrypted:	false
SSDEEP:	3:jtVmFNNAS2hETnRjSx70R:R4FMlEDhSxAR
MD5:	EDDF4AFD9D3CE9C5D57234128FA4CD0F
SHA1:	6F93430D79476D6BFF5399B739FF8ACF25CFCB31
SHA-256:	65A2D13D0B38BEAD3D51E9F9E999301935E030CC0D0F316EF9F6BC2901ACA7CA
SHA-512:	0395D7F3E4A3214BAE3BF85FB2612A9F28CCC9F9041531A9896C4843B5D4500C90939782B3D4442BB910F29C280EF4D9DC45CCE027FD1E4F45DA1AA13CD93C
Malicious:	false
Reputation:	low
Preview:	9wHh5F5EFWGRw9hKOrebnQMVAX1DfrU1/zj4/9fYO3TCqGAOjpHHJ9y6HHZF4qlc

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.138250665474018

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	QNSpfBSrsR.exe
File size:	7447752
MD5:	7da4f5e17791a774131c3c97538a2495
SHA1:	552b4a357b259935a35b06d040d7f2e3205c8e42
SHA256:	ac8ef770d70da42ea56d5b15fb5db0be89ae9250ac78b2b fd493843a50399a19
SHA512:	4c0460e29457f9910f5ebb4090fbaf1e29d28e4d2abb5f63 dbe83061cdb306e0c545db97662f6a380e438d615ad3b9 43eec8d7b1f9b57eecff63ef45557ce7b
SSDEEP:	98304:eUYsXqrhgjzKQYaqTvH6nn0GRj27SchULsKSNi T3I0jibPQMpG:FqrwaPQj2hawI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....q.....q.. ....q...@.. .....q.....ur...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0xb1a60e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FD6B4F0 [Mon Dec 14 00:42:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=US, L=New York, OU=Baedefcfddfbcecebdabbeddf, O=Aeefdaeadcceedeacdeefbeaef, CN=Debffeeacbbfccdbbc
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/14/2020 1:42:24 AM 12/14/2021 1:42:24 AM
Subject Chain	• C=US, L=New York, OU=Baedefcfddfbcecebdabbeddf, O=Aeefdaeadcceedeacdeefbeaef, CN=Debffeeacbbfccdbbc
Version:	3
Thumbprint MD5:	0357455039907173BFA3B8FD74814EF2
Thumbprint SHA-1:	DA2C9B8B17C7345CD58419DECF60533552E7F006
Thumbprint SHA-256:	86046CCE2B43DEF5D347CAD7BC5BC139E33928D0C5896D5F48B5D0318A875FAE
Serial:	00D28C58DA0E5518BB07BE5158F1D013FE

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x71a5b4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x718c00	0x18c8	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x71c000	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	0x718614	0x718800	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x71c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
mscoree.dll	_CorExeMain

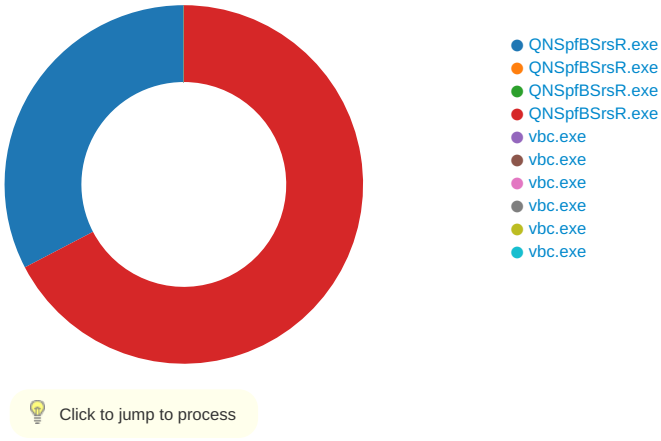
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: QNSpfBSrsR.exe PID: 6696 Parent PID: 5928

General

Start time:	20:45:39
Start date:	14/12/2020
Path:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QNSpfBSrsR.exe'
Imagebase:	0x820000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true

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	6D08CF06	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	6D08CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QNSpfBSrsR.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D39C78D	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\QNSpfBSrsR.exe.log	unknown	1039	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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.Windows.Forms, Vers	success or wait	1	6D39C907	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	6D065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CFC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D06CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CFC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CFC03DE	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	6CFC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CFC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BED1B4F	ReadFile

Analysis Process: QNSpfBSrsR.exe PID: 7128 Parent PID: 6696

General

Start time:	20:46:05
Start date:	14/12/2020
Path:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Imagebase:	0x310000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: QNSpfBSrsR.exe PID: 6384 Parent PID: 6696

General

Start time:	20:46:07
Start date:	14/12/2020
Path:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Imagebase:	0x30000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: QNSpfBSrsR.exe PID: 2800 Parent PID: 6696

General

Start time:	20:46:12
Start date:	14/12/2020
Path:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QNSpfBSrsR.exe
Imagebase:	0x7f0000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1020981161.000000000358C000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.1017545701.000000000328D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.1017545701.000000000328D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000003.727612080.0000000004A15000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_M00nD3vLogger, Description: Yara detected M00nD3v Logger, Source: 00000008.00000002.1017388940.0000000003211000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1017907114.0000000003343000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.1014445392.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.1014445392.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000008.00000002.1017257384.0000000003090000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1017257384.0000000003090000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1019556248.000000000347F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1021020173.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1019524329.0000000003462000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.1021102525.0000000004211000.00000004.00000001.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	6D08CF06	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	6D08CF06	unknown
C:\Users\user\AppData\Local\Temp\2c99a7ed-ddac-ab7c-0bfe-56058ec17ef8	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BED1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9C48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9C49.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp989B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9CC3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp8FAF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp9398.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BED7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9C48.tmp	success or wait	1	6BED6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9C49.tmp	success or wait	1	6BED6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp989B.tmp	success or wait	1	6BED6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9CC3.tmp	success or wait	1	6BED6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2c99a7ed-ddac-ab7c-0bfe-56058ec17ef8	unknown	64	39 77 48 68 35 46 35 45 46 57 47 52 77 39 68 4b 4f 72 65 62 6e 51 4d 56 41 58 31 44 66 72 55 31 2f 7a 6a 34 2f 39 66 59 4f 33 54 43 71 47 41 4f 6a 70 48 48 4a 39 79 36 48 48 5a 46 34 71 6c 63	9wHh5F5EFWGRw9hKOrebnQMVAX1DfrU1/zj4/9fYO3TCqGAOjpHHJ9y6HHZF4qlc	success or wait	1	6BED1B4F	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	6D065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CFC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D06CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D065705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D065705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CFC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CFC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CFC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CFC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BED1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	2	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9C48.tmp	unknown	4096	end of file	54	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9C49.tmp	unknown	4096	end of file	59	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp989B.tmp	unknown	4096	end of file	59	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9CC3.tmp	unknown	4096	end of file	57	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8FAF.tmp	unknown	4096	end of file	1	6BED1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9398.tmp	unknown	4096	end of file	1	6BED1B4F	ReadFile

Analysis Process: vbc.exe PID: 4204 Parent PID: 2800

General

Start time:	20:46:18

Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9C49.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000A.00000002.739382606.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000002.739382606.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 5732 Parent PID: 2800

General

Start time:	20:46:18
Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9C48.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000B.00000002.739399669.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.739399669.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 7132 Parent PID: 2800

General

Start time:	20:47:22
Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp989B.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000F.00000002.876231898.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.876231898.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 7012 Parent PID: 2800

General

Start time:	20:47:23
Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9CC3.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000010.00000002.878633274.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000010.00000002.878633274.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 4088 Parent PID: 2800

General

Start time:	20:48:25
Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp8FAF.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000002.1011864489.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.1011864489.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 1072 Parent PID: 2800

General

Start time:	20:48:26

Start date:	14/12/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9398.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000014.00000002.1014010873.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000014.00000002.1014010873.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis