



ID: 694560
Sample Name: IJr8RvvhZ3.exe
Cookbook: default.jbs
Time: 23:50:56
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report IJr8RvvhZ3.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 5
Initial Sample 5
Dropped Files 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Spam, unwanted Advertisements and Ransom Demands 6
System Summary 6
Data Obfuscation 7
Boot Survival 7
Malware Analysis System Evasion 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 17
Rich Headers 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Exports 19
Possible Origin 19
Network Behavior 19
UDP Packets 19
DNS Queries 20
Statistics 20
Behavior 20
System Behavior 21
Analysis Process: IJr8RvvhZ3.exePID: 732, Parent PID: 5500 21
General 21
File Activities 21
File Created 21
File Written 21
File Read 22

Registry Activities 22
Key Value Created 22
Analysis Process: mqsmvj.exePID: 4652, Parent PID: 3320 22
General 22
File Activities 23
File Read 23
Registry Activities 23
Key Value Created 23
Analysis Process: mqsmvj.exePID: 476, Parent PID: 3320 23
General 23
File Activities 24
File Read 24
Registry Activities 24
Key Value Created 24
Analysis Process: mqsmvj.exePID: 5964, Parent PID: 3320 24
General 24
File Activities 25
File Read 25
Registry Activities 25
Key Value Created 25
Analysis Process: mqsmvj.exePID: 5524, Parent PID: 3320 25
General 25
File Activities 25
File Read 25
Registry Activities 25
Key Value Created 25
Analysis Process: mqsmvj.exePID: 3824, Parent PID: 3320 26
General 26
Analysis Process: mqsmvj.exePID: 5304, Parent PID: 3320 26
General 26
File Activities 26
File Read 27
Registry Activities 27
Key Value Created 27
Analysis Process: mqsmvj.exePID: 4828, Parent PID: 3320 27
General 27
File Activities 27
File Read 27
Registry Activities 27
Key Value Created 27
Analysis Process: mqsmvj.exePID: 2228, Parent PID: 3320 28
General 28
Analysis Process: mqsmvj.exePID: 244, Parent PID: 3320 28
General 28
File Activities 28
File Read 28
Registry Activities 29
Key Value Created 29
Analysis Process: mqsmvj.exePID: 4940, Parent PID: 3320 29
General 29
File Activities 29
File Read 29
Registry Activities 29
Key Value Created 29
Analysis Process: mqsmvj.exePID: 4864, Parent PID: 3320 29
General 29
Analysis Process: mqsmvj.exePID: 5160, Parent PID: 3320 30
General 30
Analysis Process: mqsmvj.exePID: 5636, Parent PID: 3320 30
General 30
Analysis Process: mqsmvj.exePID: 2564, Parent PID: 3320 31
General 31
Analysis Process: mqsmvj.exePID: 4956, Parent PID: 3320 31
General 31
Analysis Process: mqsmvj.exePID: 4480, Parent PID: 3320 32
General 32
Analysis Process: mqsmvj.exePID: 5768, Parent PID: 3320 32
General 32
Analysis Process: mqsmvj.exePID: 6000, Parent PID: 3320 33
General 33
Analysis Process: mqsmvj.exePID: 916, Parent PID: 3320 33
General 33
Analysis Process: mqsmvj.exePID: 3780, Parent PID: 3320 33
General 34
Disassembly 34

Copyright Joe Security LLC 2022

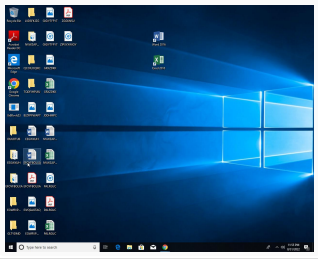
Windows Analysis Report

IJr8RvvhZ3.exe

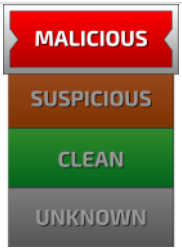
Overview

General Information

Sample Name:	IJr8RvvhZ3.exe
Analysis ID:	694560
MD5:	b77359bc85030f..
SHA1:	5bff219a3d20203.
SHA256:	afd36e5d309ba8..
Tags:	exe
Infos:	



Detection



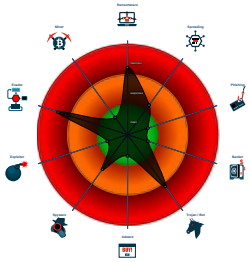
Gandcrab, ReflectiveLoader

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

Signatures

- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected ReflectiveLoader
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Creates multiple autostart registry k…
- Found evasive API chain (may stop…
- Contains functionality to determine t…
- Found Tor onion address
- Machine Learning detection for sam…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- IJr8RvvhZ3.exe (PID: 732 cmdline: "C:\Users\user\Desktop\IJr8RvvhZ3.exe" MD5: B77359BC85030F5F856B8010C0DDF6A8)
- mqsmvj.exe (PID: 4652 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 476 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5964 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5524 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 3824 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5304 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 4828 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 2228 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 244 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 4940 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 4864 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5160 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5636 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 2564 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 4956 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 4480 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 5768 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 6000 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 916 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- mqsmvj.exe (PID: 3780 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe" MD5: 937D3395BC50812DBAB14034E2FCC25B)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
IJr8RvvhZ3.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
IJr8RvvhZ3.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
IJr8RvvhZ3.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
IJr8RvvhZ3.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
IJr8RvvhZ3.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&

Click to see the 1 entries

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&

Click to see the 1 entries

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.344084967.000000000F592000.00000004.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000010.00000002.406166723.000000000F592000.00000004.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0000001C.00000000.542136140.000000000F58A000.00000002.00000001.01000000.00000006.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
0000001E.00000002.598229388.000000000F592000.00000004.00000001.01000000.00000006.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader

Click to see the 181 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
23.0.mqsmvj.exe.f580000.0.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
23.0.mqsmvj.exe.f580000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
23.0.mqsmvj.exe.f580000.0.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
23.0.mqsmvj.exe.f580000.0.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
23.0.mqsmvj.exe.f580000.0.unpack	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
Click to see the 442 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 / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Contains functionality to determine the online IP of the system

Found Tor onion address

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands



Yara detected Gandcrab

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected ReflectiveLoader

Boot Survival



Creates multiple autostart registry keys

Malware Analysis System Evasion

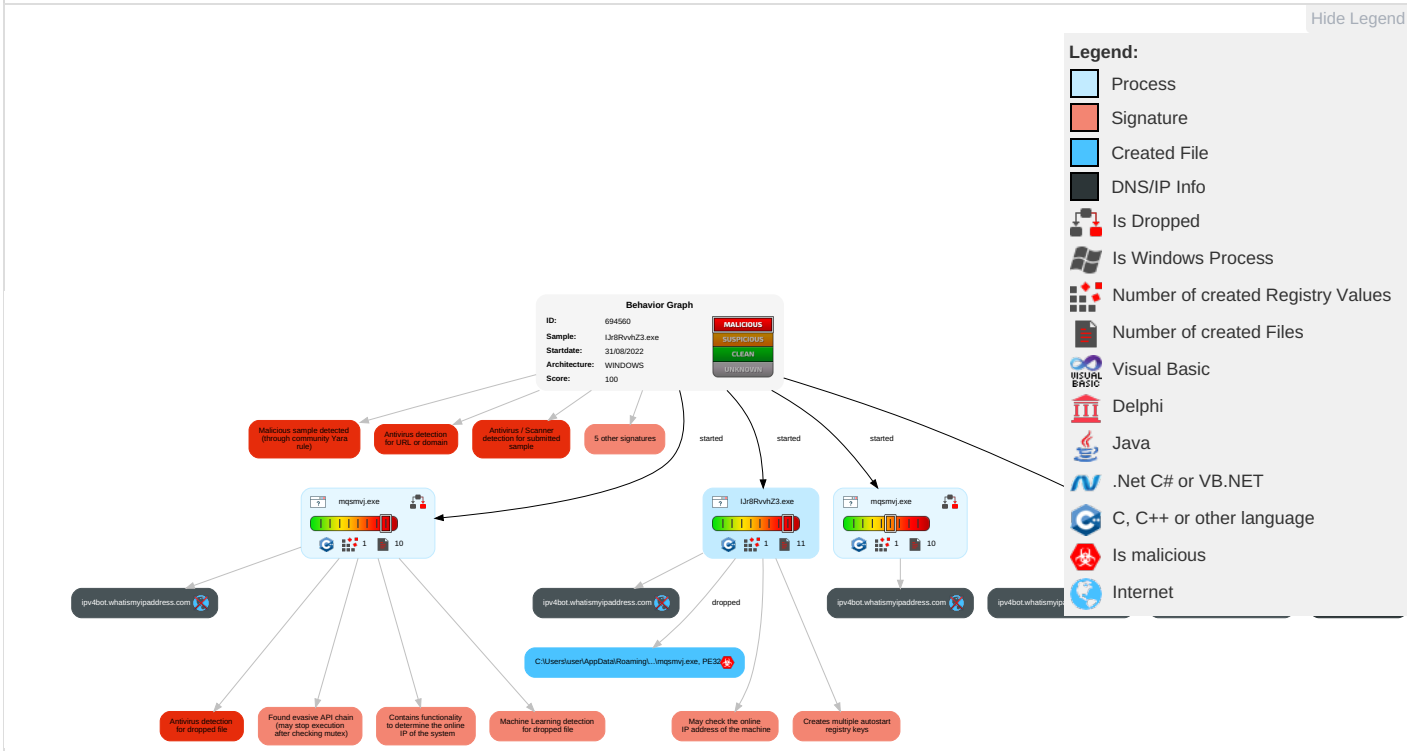


Found evasive API chain (may stop execution after checking mutex)

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
1 Replication Through Removable Media	1 1 Native API	1 1 Registry Run Keys / Startup Folder	1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Process Injection	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	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)	Binary Padding	NTDS	1 1 Peripheral Device Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Proxy	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System 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	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration 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)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 File and Directory Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	4 4 System Information Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

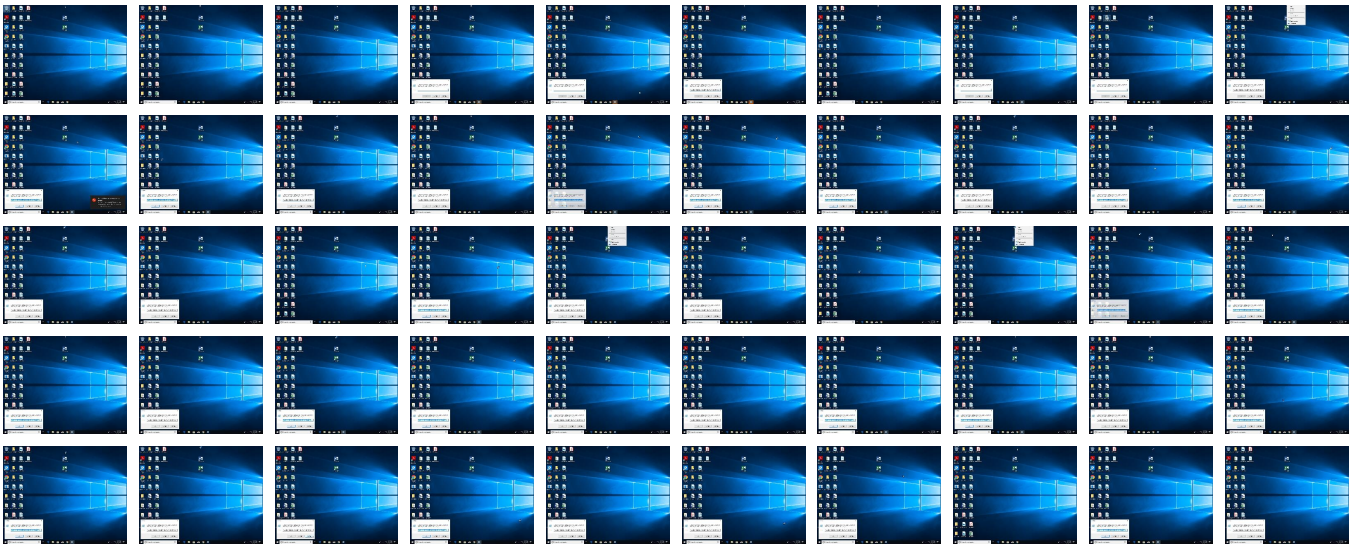
Behavior Graph

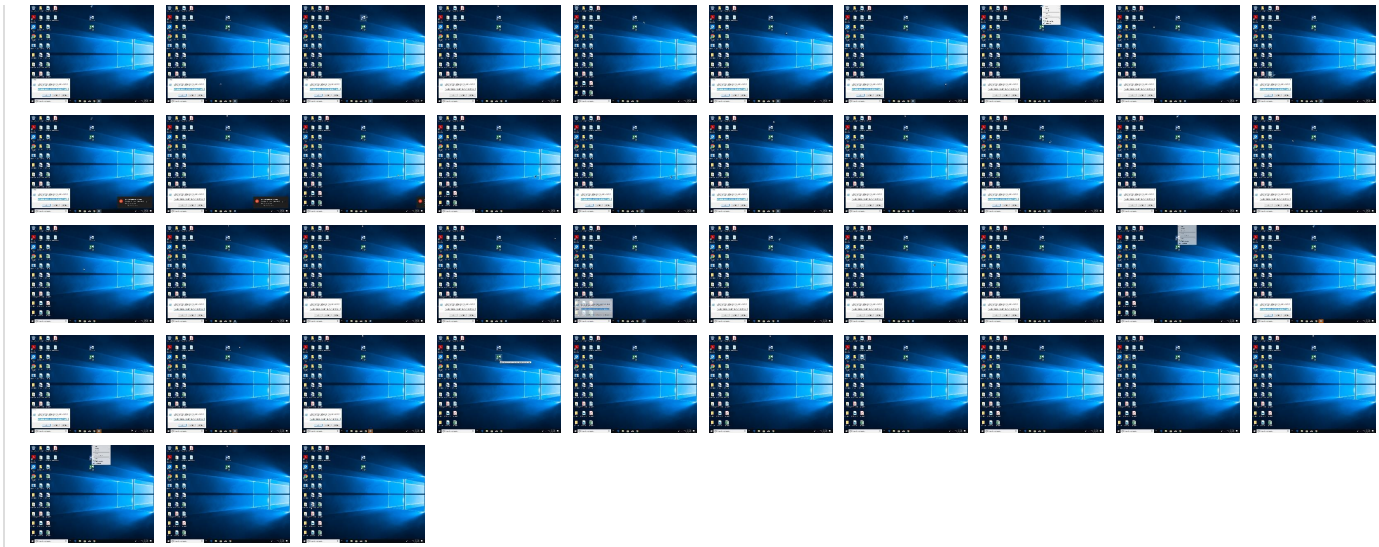


Screenshots

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
IJr8RvvhZ3.exe	87%	Virustotal		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
IJr8RvvhZ3.exe	86%	Metadefender		Browse
IJr8RvvhZ3.exe	96%	ReversingLabs	Win32.Ransomware.GandCrab	
IJr8RvvhZ3.exe	100%	Avira	TR/Dropper.Gen	
IJr8RvvhZ3.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
25.3.mqsmvj.exe.3490000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.3.mqsmvj.exe.3790000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
27.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
22.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.IJr8RvvhZ3.exe.f140000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
39.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
38.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
36.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
22.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
28.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
35.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.3.mqsmvj.exe.32b0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
28.3.mqsmvj.exe.3130000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
35.3.mqsmvj.exe.3970000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.3.mqsmvj.exe.3a70000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.3.mqsmvj.exe.3930000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
39.3.mqsmvj.exe.2fb0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
38.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.3.mqsmvj.exe.3290000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
37.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.IJr8RvvhZ3.exe.f140000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
39.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.3.mqsmvj.exe.3b50000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
27.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.3.mqsmvj.exe.2fb0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
28.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
36.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
35.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.3.mqsmvj.exe.3470000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
37.3.mqsmvj.exe.3bc0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.IJr8RvvhZ3.exe.3210000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
27.3.mqsmvj.exe.3490000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
37.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.2.mqsmvj.exe.f580000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbmuveqjsli57x.onion/63b5ce1c617217a5	100%	Avira URL Cloud	malware	
http://https://tox.chat/download.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipv4bot.whatismyipaddress.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ipv4bot.whatismyipaddress.com/a	mqsmvj.exe, 0000000C.00000002.343812574.0000000000873000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000C.00000003.343418273.0000000000873000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.torproject.org/	IJr8RvvhZ3.exe, 00000000.00000002.257994631.000000000F152000.00000004.00000001.01000000.00000003.sdmp, mqsmvj.exe, 00000003.00000002.298139854.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000B.00000002.328015412.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000C.00000002.344084967.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000E.00000002.374552502.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000010.00000002.406166723.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000013.00000002.437026618.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000017.00000002.473021592.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000019.00000002.502628191.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001B.00000002.543807830.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001C.00000002.559901286.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001E.00000002.598229388.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000023.00000002.638125851.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000025.00000002.681251272.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000027.00000002.720286366.000000000F592000.00000004.00000001.01000000.00000006.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/$	mqsmvj.exe, 0000000C.00000002.343769957.0000000000838000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/4	mqsmvj.exe, 0000000C.00000002.343812574.0000000000873000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000C.00000003.343418273.0000000000873000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/CwX	mqsmvj.exe, 0000000E.00000002.373523162.0000000000AD8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://gdcbmuveqjsli57x.onion/63b5ce1c617217a5	IJr8RvvhZ3.exe, 00000000.00000002.257994631.000000000F152000.00000004.00000001.01000000.00000003.sdmp, mqsmvj.exe, 00000003.00000002.298139854.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000B.00000002.328015412.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000C.00000002.344084967.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000E.00000002.374552502.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000010.00000002.406166723.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000013.00000002.437026618.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000017.00000002.473021592.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000019.00000002.502628191.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001B.00000002.543807830.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001C.00000002.559901286.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001E.00000002.598229388.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000023.00000002.638125851.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000025.00000002.681251272.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000027.00000002.720286366.000000000F592000.00000004.00000001.01000000.00000006.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ipv4bot.whatismyipaddress.com/9I)	mqsmvj.exe, 00000019.00000002.501583638.0000000000D18000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/I	mqsmvj.exe, 0000000B.00000002.327597151.000000000093A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	mqsmvj.exe, 0000000B.00000002.327597151.000000000093A000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000C.00000002.343812574.0000000000873000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000C.00000003.343418273.00000000873000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000C.00000002.343769957.0000000000838000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 0000000E.00000002.373523162.0000000000AD8000.00000004.00000020.00020000.00000000.sdmp, mqsmvj.exe, 00000019.00000002.501583638.0000000000D18000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://tox.chat/download.html	IJr8RvvhZ3.exe, 00000000.00000002.257994631.000000000F152000.00000004.00000001.01000000.00000003.sdmp, mqsmvj.exe, 00000003.00000002.298139854.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000B.00000002.328015412.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000C.00000002.344084967.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000000E.00000002.374552502.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000010.00000002.406166723.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000013.00000002.437026618.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000017.00000002.473021592.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000019.00000002.502628191.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001B.00000002.543807830.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001C.00000002.559901286.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 0000001E.00000002.598229388.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000023.00000002.638125851.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000025.00000002.681251272.000000000F592000.00000004.00000001.01000000.00000006.sdmp, mqsmvj.exe, 00000027.00000002.720286366.000000000F592000.00000004.00000001.01000000.00000006.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694560
Start date and time:	2022-08-31 23:50:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IJr8RvvhZ3.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:	40
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.rans.troj.evad.winEXE@21/1@15/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99% (good quality ratio 95.1%) • Quality average: 83% • Quality standard deviation: 24.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:52:02	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce qwipuxgrdpk "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:52:12	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce qwipuxgrdpk "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:52:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce tlrxymtwiqr "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:52:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce soasnzfwfwv "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:52:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce xxjrkojdmxk "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:52:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce xbugmifmcap "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce tlrxymtwiqr "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce soasnzfwfwv "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce xxjrkojdmxk "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce xbugmifmcap "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce bahswixbtvj "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:53:49	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce dpmkfuaielt "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:54:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce eeukvfrmhuc "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"

Copyright Joe Security LLC 2022

Time	Type	Description
23:54:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce yzthpvkcmuu "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:54:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ponrvbljnrm "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:54:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce bahswixbtvj "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:54:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce dpmkfuaielt "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:54:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce eeukvfrmhuc "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:55:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce yzthpvkcmuu "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
23:55:12	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ponrvbljnrm "C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"

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\Roaming\Microsoft\mqsmvj.exe

Process:	C:\Users\user\Desktop\IJr8RvvhZ3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	71680
Entropy (8bit):	6.490172186221231
Encrypted:	false
SSDEEP:	1536:VZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:Ed5BJHMqqDL2/Ovvdr
MD5:	937D3395BC50812DBAB14034E2FCC25B
SHA1:	DB221BDAAE201CD4CD39EC97CE6FA933DA9FACFB
SHA-256:	B34EF0C18F05108E829F41196C84E5A9C93FBB4C03D61CF42BB277AC1D1A7ABA
SHA-512:	02EFC4F8FBAEF139B392AE60F8678CBCC1C84761F80CBA3642DCF519D06B1FF63D1499917B8A50424F6EAF54E6141D513DB1D2D42730EED4192BB0EC1D7A546D
Malicious:	**true**

Yara Hits:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This (..X..m cannot be run in DOS mode....$.....}.....B.....B.....1.....Y...G.....~.....y.....|....Rich..... ...PE..L....6.Z..... K.....Z..... ....@.....P...U.....@.....P..... ..text...H..... ..`.rdata..&q.....r.....@..@.data..... .....@....CRT.....0.....@..@.rsrc.....@.....@..@.reloc.....P..... .....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.4901978767924895
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	IJr8RvvhZ3.exe
File size:	71680
MD5:	b77359bc85030f5f856b8010c0ddf6a8
SHA1:	5bff219a3d20203a239a23db69385f2611e67f5d
SHA256:	afd36e5d309ba8576b7e6a31ab1b3af4c3c0530052a2c31b97c688c0e2515005
SHA512:	c0dc63351d03b120a3b20b31596c0d4235fa4ef4d8228d01450486f73226cc40ab357d5050a24e51c4783cfc55f005e59d8fb8e73644beae0590554a3efbe829
SSDEEP:	1536:sZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:zd5BJHMqqDL2/Ovvdr
TLSH:	1A636C1DB2D1B293F1E396B9FAB57E25445D2D103B056BEB08A369F568120F16C3B703
File Content Preview:	MZ.....@.....!..L.!This .....m cannot be run in DOS mode....$.....}.....B.....B.....1.....Y.....G.....~.....y.....|.....Rich.....PE..L..

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x10004b20
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x5A9C3687 [Sun Mar 4 18:10:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1

Import Hash:	8735e6cad23590d9b5b60978db488a28

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 4Ch
push 000003E8h
call dword ptr [1000A098h]
call 00007FD018C883BFh
test eax, eax
je 00007FD018C8872Ah
push 00000000h
call dword ptr [1000A168h]
push 00000000h
push 00000000h
push 00000000h
push 10002D30h
push 00000000h
push 00000000h
call dword ptr [1000A108h]
mov dword ptr [ebp-04h], eax
cmp dword ptr [ebp-04h], 00000000h
je 00007FD018C8874Eh
push 00001388h
mov eax, dword ptr [ebp-04h]
push eax
call dword ptr [1000A080h]
cmp eax, 00000102h
jne 00007FD018C8872Eh
push 00000000h
mov ecx, dword ptr [ebp-04h]
push ecx
call dword ptr [1000A094h]
mov edx, dword ptr [ebp-04h]
push edx
call dword ptr [1000A10Ch]
call 00007FD018C88454h
call 00007FD018C87E3Fh
lea ecx, dword ptr [ebp-4Ch]
call 00007FD018C8A0D7h
mov dword ptr [ebp-24h], 00000000h
mov dword ptr [ebp-20h], 00000000h
mov dword ptr [ebp-18h], 00000000h
mov dword ptr [ebp-28h], 00000000h
lea eax, dword ptr [ebp-20h]
push eax
lea ecx, dword ptr [ebp-24h]
push ecx
lea edx, dword ptr [ebp-28h]
push edx
lea eax, dword ptr [ebp-18h]
push eax
lea ecx, dword ptr [ebp-4Ch]
call 00007FD018C8A053h
mov dword ptr [ebp-2Ch], 00000000h
mov dword ptr [ebp-0Ch], 00000000h
mov ecx, dword ptr [ebp-18h]
call 00007FD018C8863Dh

Copyright Joe Security LLC 2022

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2013 build 21005 • [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x10550	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x105a8	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15000	0xaf4	.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	0xa000	0x200	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8448	0x8600	False	0.4546991604477612	data	6.32052618210059	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x7126	0x7200	False	0.47765899122807015	data	6.1644872822657275	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0xa84	0xc00	False	0.3056640625	data	3.538638851099626	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x13000	0x4	0x200	False	0.033203125	data	0.04078075625387198	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1e0	0x200	False	0.52734375	data	4.7176788329467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15000	0xaf4	0xc00	False	0.7932942708333334	data	6.537931848954439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x14060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	ReadFile, SetFilePointer, GetFileAttributesW, GetLastError, MoveFileW, lstrcpyW, SetFileAttributesW, CreateMutexW, GetDriveTypeW, VerSetConditionMask, WaitForSingleObject, GetTickCount, InitializeCriticalSection, OpenProcess, GetSystemDirectoryW, TerminateThread, Sleep, TerminateProcess, VerifyVersionInfoW, WaitForMultipleObjects, DeleteCriticalSection, ExpandEnvironmentStringsW, lstrlenW, SetHandleInformation, lstrcatA, MultiByteToWideChar, CreatePipe, lstrcmpiA, Process32NextW, CreateToolhelp32Snapshot, LeaveCriticalSection, EnterCriticalSection, FindFirstFileW, lstrcmpW, FindClose, FindNextFileW, GetNativeSystemInfo, GetComputerNameW, GetDiskFreeSpaceW, GetWindowsDirectoryW, GetVolumeInformationW, LoadLibraryA, lstrcmpiW, VirtualFree, CreateThread, CloseHandle, lstrcatW, CreateFileMappingW, ExitThread, CreateFileW, GetModuleFileNameW, WriteFile, GetModuleHandleW, UnmapViewOfFile, MapViewOfFile, GetFileSize, GetEnvironmentVariableW, lstrcpyA, GetModuleHandleA, VirtualAlloc, GetProcAddress, Process32FirstW, GetTempPathW, GetProcessHeap, HeapFree, HeapAlloc, lstrlenA, CreateProcessW, ExitProcess, IsProcessorFeaturePresent

DLL	Import
USER32.dll	BeginPaint, wsprintfW, TranslateMessage, LoadCursorW, LoadIconW, MessageBoxA, GetMessageW, EndPaint, DestroyWindow, RegisterClassExW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, wsprintfA, GetForegroundWindow, SetWindowLongW
GDI32.dll	TextOutW
ADVAPI32.dll	FreeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptExportKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, AllocateAndInitializeSid
SHELL32.dll	ShellExecuteW, SHGetSpecialFolderPathW, ShellExecuteExW
CRYPT32.dll	CryptStringToBinaryA, CryptBinaryToStringA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

Exports

Name	Ordinal	Address
_ReflectiveLoader@0	1	0x10005ff0

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:52:00.770551920 CEST	50835	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:52:00.789747953 CEST	53	50835	8.8.8.8	192.168.2.7
Aug 31, 2022 23:52:19.089329004 CEST	63926	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:52:19.109457970 CEST	53	63926	8.8.8.8	192.168.2.7
Aug 31, 2022 23:52:29.696835041 CEST	53336	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:52:29.716440916 CEST	53	53336	8.8.8.8	192.168.2.7
Aug 31, 2022 23:52:40.983445883 CEST	50513	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:52:41.002794027 CEST	53	50513	8.8.8.8	192.168.2.7
Aug 31, 2022 23:52:54.908077955 CEST	65356	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:52:54.927706003 CEST	53	65356	8.8.8.8	192.168.2.7
Aug 31, 2022 23:53:08.850558043 CEST	51526	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:53:08.868645906 CEST	53	51526	8.8.8.8	192.168.2.7
Aug 31, 2022 23:53:24.176354885 CEST	58784	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:53:24.195504904 CEST	53	58784	8.8.8.8	192.168.2.7
Aug 31, 2022 23:53:40.707055092 CEST	64608	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:53:40.724586010 CEST	53	64608	8.8.8.8	192.168.2.7
Aug 31, 2022 23:53:54.471183062 CEST	58746	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:53:54.489445925 CEST	53	58746	8.8.8.8	192.168.2.7
Aug 31, 2022 23:54:13.856695890 CEST	61248	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:54:13.874511003 CEST	53	61248	8.8.8.8	192.168.2.7
Aug 31, 2022 23:54:21.065799952 CEST	52750	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:54:21.085493088 CEST	53	52750	8.8.8.8	192.168.2.7
Aug 31, 2022 23:54:39.098484993 CEST	59053	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:54:39.117619038 CEST	53	59053	8.8.8.8	192.168.2.7
Aug 31, 2022 23:54:57.904921055 CEST	62018	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:54:57.924809933 CEST	53	62018	8.8.8.8	192.168.2.7
Aug 31, 2022 23:55:17.357094049 CEST	64322	53	192.168.2.7	8.8.8.8
Aug 31, 2022 23:55:17.374757051 CEST	53	64322	8.8.8.8	192.168.2.7
Aug 31, 2022 23:55:35.095211029 CEST	50197	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:55:35.114885092 CEST	53	50197	8.8.8.8	192.168.2.7

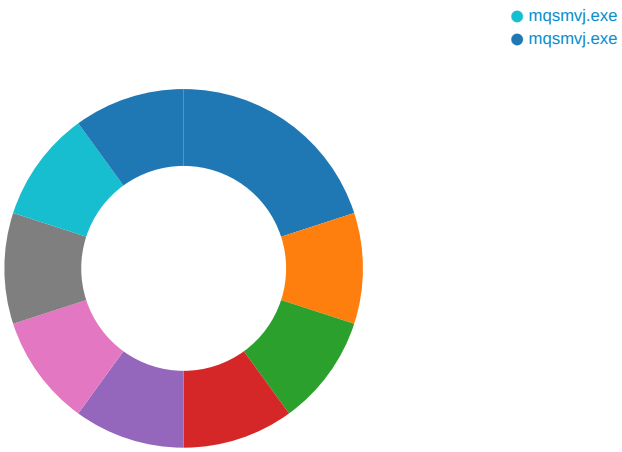
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:52:00.770551920 CEST	192.168.2.7	8.8.8.8	0x2ba7	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:52:19.089329004 CEST	192.168.2.7	8.8.8.8	0x47b1	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:52:29.696835041 CEST	192.168.2.7	8.8.8.8	0x3121	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:52:40.983445883 CEST	192.168.2.7	8.8.8.8	0x13cc	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:52:54.908077955 CEST	192.168.2.7	8.8.8.8	0x6518	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:08.850558043 CEST	192.168.2.7	8.8.8.8	0x23bf	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:24.176354885 CEST	192.168.2.7	8.8.8.8	0x9133	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:40.707055092 CEST	192.168.2.7	8.8.8.8	0x61b6	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:54.471183062 CEST	192.168.2.7	8.8.8.8	0x6884	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:13.856695890 CEST	192.168.2.7	8.8.8.8	0xbbd6	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:21.065799952 CEST	192.168.2.7	8.8.8.8	0xea49	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:39.098484993 CEST	192.168.2.7	8.8.8.8	0xf3b1	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:57.904921055 CEST	192.168.2.7	8.8.8.8	0x55f7	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:55:17.357094049 CEST	192.168.2.7	8.8.8.8	0x1c7	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:55:35.095211029 CEST	192.168.2.7	8.8.8.8	0x597e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)

Statistics

Behavior





System Behavior

Analysis Process: IJr8RvvhZ3.exe PID: 732, Parent PID: 5500

General

Target ID:	0
Start time:	23:51:54
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\IJr8RvvhZ3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\IJr8RvvhZ3.exe"
Imagebase:	0xf140000
File size:	71680 bytes
MD5 hash:	B77359BC85030F5F856B8010C0DDF6A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.246598852.000000000F14A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.257994631.000000000F152000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.257988090.000000000F14A000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000000.00000003.257187894.0000000003210000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F142852	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	0	71680	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

Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000002.298139854.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000000.284909876.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000002.298127638.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000003.00000003.296444653.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe, Author: ReversingLabs
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	tlrxymtwiqr	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **476**, Parent PID: **3320**

General

Target ID:	11
Start time:	23:52:20
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000B.00000000.302753635.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000B.00000003.321306914.0000000003290000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000B.00000002.328006726.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000B.00000002.328015412.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	soasnzfwfwv	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: 5964, Parent PID: 3320

General

Target ID:	12
Start time:	23:52:29
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000C.00000002.344084967.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000002.344076256.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000000.326861802.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000C.00000003.343391224.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	xxjrkojdmxk	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **5524**, Parent PID: **3320**

General

Target ID:	14
Start time:	23:52:40
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000002.374541763.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000E.00000003.373224342.00000000032B0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000000.345391884.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000E.00000002.374552502.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	xbugmifmcap	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **3824**, Parent PID: **3320**

General

Target ID:	15
Start time:	23:52:49
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000002.373855926.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000000.366415830.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **5304**, Parent PID: **3320**

General

Target ID:	16
Start time:	23:52:59
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000010.00000002.406166723.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000010.00000000.384391365.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000010.00000002.406139264.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000010.00000003.403183321.0000000003B50000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	bahswixbtvj	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **4828**, Parent PID: **3320**

General

Target ID:	19
Start time:	23:53:13
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000000.415482571.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000013.00000003.435943163.0000000003930000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000013.00000002.437026618.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000002.436990656.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	dpmkfuaielt	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **2228**, Parent PID: **3320**

General

Target ID:	22
Start time:	23:53:22
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000002.437171123.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000000.433686067.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **244**, Parent PID: **3320**

General

Target ID:	23
Start time:	23:53:30
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000017.00000003.471429233.0000000003A70000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000017.00000002.473021592.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000002.472905613.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000000.455550683.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Copyright Joe Security LLC 2022

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	eeukvfrmhuc	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **4940**, Parent PID: **3320**

General

Target ID:	25
Start time:	23:53:40
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000019.00000003.501007155.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000000.473313238.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000002.502607674.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000019.00000002.502628191.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe	unknown	71680	success or wait	1	F583652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	yzthpvkcmuu	unicode	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"	success or wait	1	F582AAA	RegSetValueExW

Analysis Process: mqsmvj.exe PID: **4864**, Parent PID: **3320**

General

Target ID:	26

Start time:	23:53:49
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001A.00000000.495173424.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001A.00000002.502804269.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **5160**, Parent PID: **3320**

General

Target ID:	27
Start time:	23:54:01
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001B.00000002.543716929.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001B.00000000.518024199.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001B.00000003.542421272.0000000003490000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001B.00000002.543807830.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **5636**, Parent PID: **3320**

General

Target ID:	28
Start time:	23:54:10
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001C.00000000.542136140.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001C.00000002.559901286.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001C.00000002.559852565.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001C.00000003.557904847.0000000003130000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: mqsmvj.exe PID: **2564**, Parent PID: **3320**

General

Target ID:	30
Start time:	23:54:21
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001E.00000002.598229388.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000002.598200905.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000000.560904578.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001E.00000003.596521661.0000000003470000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: mqsmvj.exe PID: **4956**, Parent PID: **3320**

General

Target ID:	34
Start time:	23:54:30
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000

File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000022.00000000.583307214.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000022.00000002.593533053.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **4480**, Parent PID: **3320**

General

Target ID:	35
Start time:	23:54:43
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0x7ff72dbc0000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000023.00000000.607979017.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000023.00000002.638125851.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000023.00000002.638106882.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000023.00000003.636841128.0000000003970000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: mqsmvj.exe PID: **5768**, Parent PID: **3320**

General

Target ID:	36
Start time:	23:54:52
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000024.00000002.634796069.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000024.00000000.631210947.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **6000**, Parent PID: **3320**

General

Target ID:	37
Start time:	23:55:02
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000025.00000002.681141144.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000025.00000000.650224978.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000025.00000003.678519196.0000000003BC0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000025.00000002.681251272.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **916**, Parent PID: **3320**

General

Target ID:	38
Start time:	23:55:12
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000026.00000002.678365276.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000026.00000000.674598119.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mqsmvj.exe PID: **3780**, Parent PID: **3320**

General	
Target ID:	39
Start time:	23:55:23
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\mqsmvj.exe"
Imagebase:	0xf580000
File size:	71680 bytes
MD5 hash:	937D3395BC50812DBAB14034E2FCC25B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000027.00000000.693057490.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000027.00000002.720286366.000000000F592000.00000004.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000027.00000002.720225413.000000000F58A000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000027.00000003.716539661.0000000002FB0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Disassembly

No disassembly