ID: 551470
Sample Name: RFQ_GGMC-Ref 12-01-2022.exe
Cookbook: default.jbs
Time: 09:01:01
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

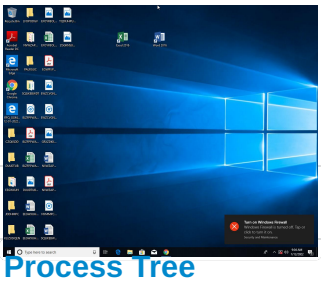
Windows Analysis Report RFQ_GGMC-Ref 12-01-2022.e…

Overview

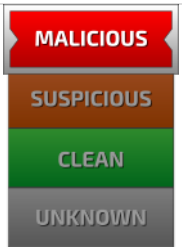
General Information

Sample Name:	RFQ_GGMC-Ref 12-01-2022.exe
Analysis ID:	551470
MD5:	9fd45110bad75cd.
SHA1:	a43016fa816afd1..
SHA256:	b586ca95ba9557..
Tags:	AsyncRAT exe
Infos:	

Most interesting Screenshot:



Detection



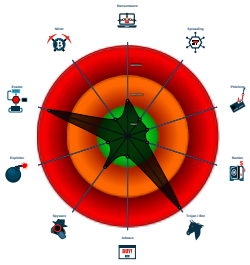
AgentTesla
AsyncRAT Nanocore

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

Signatures

- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected AsyncRAT
- Yara detected Nanocore RAT
- Sigma detected: Suspicious Script E…
- Bypasses PowerShell execution pol…
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…

Classification



Process Tree

- **System is w10x64**
- RFQ_GGMC-Ref 12-01-2022.exe (PID: 6964 cmdline: "C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe" MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
  - powershell.exe (PID: 6080 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6136 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lhWbLvHNlciwu" /XML "C:\Users\user\AppData\Local\Temp\tmp71CD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RFQ_GGMC-Ref 12-01-2022.exe (PID: 7000 cmdline: C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
  - RFQ_GGMC-Ref 12-01-2022.exe (PID: 6948 cmdline: C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
    - cmd.exe (PID: 5684 cmdline: "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "mozille" /tr "'C:\Users\user\AppData\Local\Temp\mozille.exe'" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5580 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "mozille" /tr "'C:\Users\user\AppData\Local\Temp\mozille.exe'" MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 3868 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmpB8D1.tmp.bat"" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - conhost.exe (PID: 2532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 2292 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - mozille.exe (PID: 6564 cmdline: "C:\Users\user\AppData\Local\Temp\mozille.exe" MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
        - powershell.exe (PID: 5452 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- mozille.exe (PID: 6316 cmdline: C:\Users\user\AppData\Local\Temp\mozille.exe MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
  - powershell.exe (PID: 5400 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5192 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lhWbLvHNlciwu" /XML "C:\Users\user\AppData\Local\Temp\tmpCDE7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mozille.exe (PID: 6620 cmdline: C:\Users\user\AppData\Local\Temp\mozille.exe MD5: 9FD45110BAD75CDA6DE67232014AEB6E)
    - cmd.exe (PID: 5000 cmdline: "C:\Windows\System32\cmd.exe" /c start /b powershell ExecutionPolicy Bypass Start-Process -FilePath "'C:\Users\user\AppData\Local\Temp\jzhlgt.exe'" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5648 cmdline: powershell ExecutionPolicy Bypass Start-Process -FilePath "'C:\Users\user\AppData\Local\Temp\jzhlgt.exe'" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - jzhlgt.exe (PID: 6500 cmdline: "C:\Users\user\AppData\Local\Temp\jzhlgt.exe" MD5: 76F7AB6A302E47D7F7FDB4EA2540323E)
          - jzhlgt.exe (PID: 5964 cmdline: C:\Users\user\AppData\Local\Temp\jzhlgt.exe MD5: 76F7AB6A302E47D7F7FDB4EA2540323E)
          - jzhlgt.exe (PID: 3076 cmdline: C:\Users\user\AppData\Local\Temp\jzhlgt.exe MD5: 76F7AB6A302E47D7F7FDB4EA2540323E)
    - cmd.exe (PID: 3312 cmdline: "C:\Windows\System32\cmd.exe" /c start /b powershell ExecutionPolicy Bypass Start-Process -FilePath "'C:\Users\user\AppData\Local\Temp\dlliok.exe'" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 4636 cmdline: powershell ExecutionPolicy Bypass Start-Process -FilePath "'C:\Users\user\AppData\Local\Temp\dlliok.exe'" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - dlliok.exe (PID: 2804 cmdline: "C:\Users\user\AppData\Local\Temp\dlliok.exe" MD5: 8B4D4FC3E962F26A4C74120F33BB7460)
          - powershell.exe (PID: 6276 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\pLrWNKFD.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - schtasks.exe (PID: 4872 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\pLrWNKFD" /XML "C:\Users\user\AppData\Local\Temp\tmp9C7F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 4740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - dlliok.exe (PID: 1316 cmdline: C:\Users\user\AppData\Local\Temp\dlliok.exe MD5: 8B4D4FC3E962F26A4C74120F33BB7460)
            - schtasks.exe (PID: 4412 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpAD4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
              - conhost.exe (PID: 6124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dlliok.exe (PID: 6844 cmdline: C:\Users\user\AppData\Local\Temp\dlliok.exe 0 MD5: 8B4D4FC3E962F26A4C74120F33BB7460)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000028.00000002.578366682.000000000552 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000028.00000002.578366682.000000000552 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000001D.00000000.485797688.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001D.00000000.485797688.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000015.00000002.564363154.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 64 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.10.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.4.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.6.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
7.2.RFQ_GGMC-Ref 12-01-2022.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.12.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 6 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected Costura Assembly Loader

Suspicious powershell command line found

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival:

Yara detected AsyncRAT

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Yara detected AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion:

Bypasses PowerShell execution policy

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected Nanocore RAT

Remote Access Functionality:

Yara detected Telegram RAT

Yara detected AgentTesla

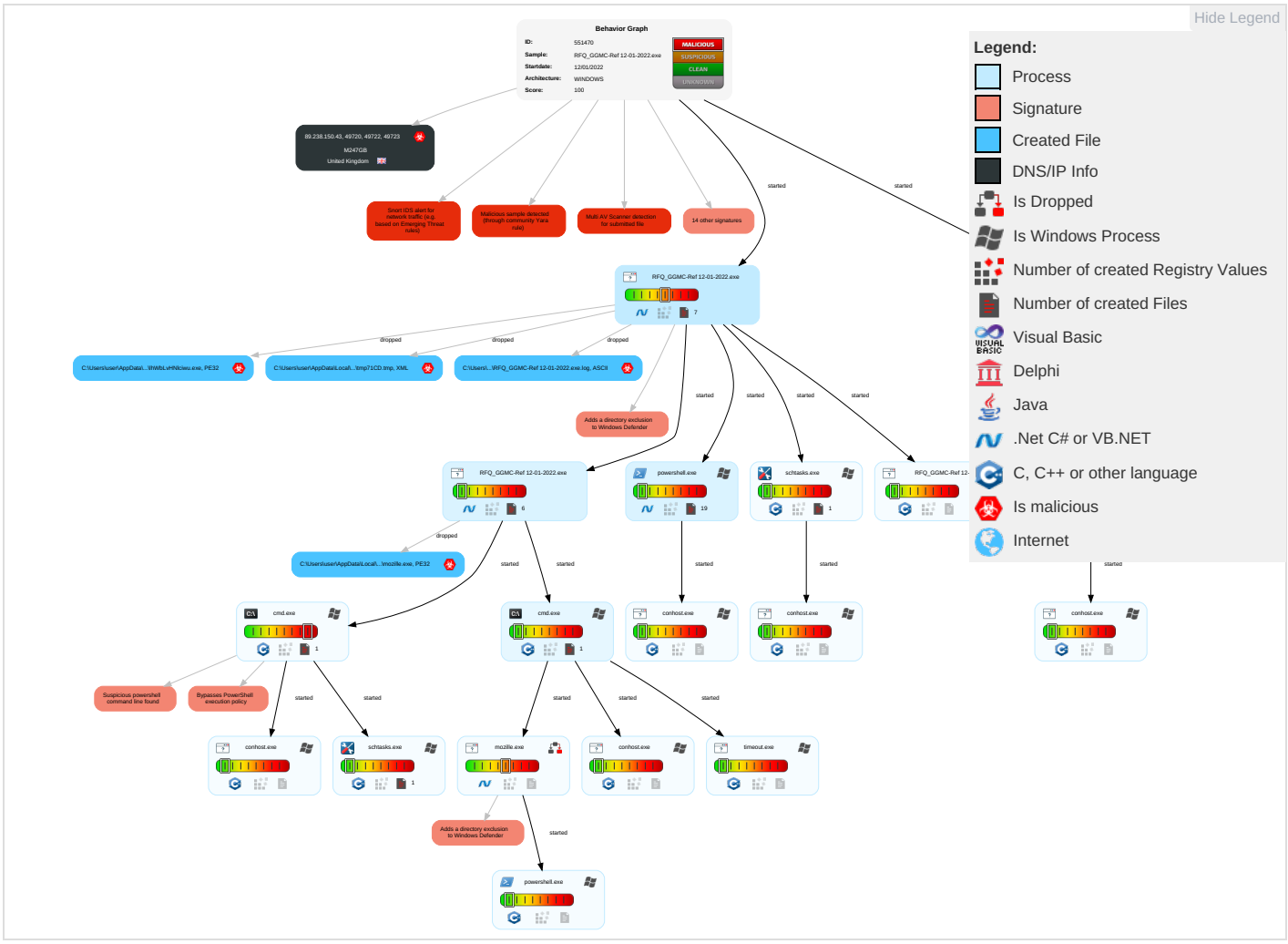
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 2	Scheduled Task/Job 2	Process Injection 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 2	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	PowerShell 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

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
RFQ_GGMC-Ref 12-01-2022.exe	26%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.RFQ_GGMC-Ref 12-01-2022.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.12.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.RFQ_GGMC-Ref 12-01-2022.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://micolous.id.au/projects/bf21	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.totalbf2142.com/forums/showthread.php?t=5342	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://micolous.id.au/projects/bf2142/.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://micolous.id.au	0%	Avira URL Cloud	safe	
http://micolous.id.au/projects/bf2142/	0%	Avira URL Cloud	safe	
http://igaeJZ.so	0%	Avira URL Cloud	safe	
http://www.pcgamingboards.com/smf/index.php?topic=129.msg279#msg279	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://micolous.id.au/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.238.150.43	unknown	United Kingdom		9009	M247GB	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551470
Start date:	12.01.2022
Start time:	09:01:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ_GGMC-Ref 12-01-2022.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@53/16@0/1
EGA Information:	• Successful, ratio: 60%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0%) • Quality average: 12.9% • Quality standard deviation: 33.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:02:09	API Interceptor	1x Sleep call for process: RFQ_GGMC-Ref 12-01-2022.exe modified
09:02:13	API Interceptor	138x Sleep call for process: powershell.exe modified
09:02:31	Task Scheduler	Run new task: mozille path: "C:\Users\user\AppData\Local\Temp\mozille.exe"
09:02:37	API Interceptor	4x Sleep call for process: mozille.exe modified
09:03:24	API Interceptor	164x Sleep call for process: jzhlgt.exe modified
09:03:41	API Interceptor	33x Sleep call for process: dlliok.exe modified
09:03:59	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\dlliok.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ_GGMC-Ref 12-01-2022.exe.log	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mozille.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\mozille.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Category:	dropped
Size (bytes):	21704
Entropy (8bit):	5.597528400509029
Encrypted:	false
SSDEEP:	384:/tL67waWub8VWzZPWCDzj8eNSBKnsjultlW8aepEQt11u16z+5mHKHVg3P8j6lvv:4CubLz5FfN4KsClt8a+f13+U+WEmlc
MD5:	2F13EF84B063265B6634CB005F4B5286
SHA1:	0AA0F7DC07BD5D1A12DAE304E40B70755A3F164A
SHA-256:	638143E39E07AD1C5DAF1BE1FB96B03C42B543B790849C7716AC2AC6718F667E
SHA-512:	9CBD81D15290642E4853B32BAAC634395AAC24B40279E8D24C33715EDA4161FE45580BA39C97CC8295B2CE312E97251795542323795ED32F74F9774B7E0CC4AD
Malicious:	false
Reputation:	unknown
Preview:	@...e.....u.P.E.B... .l.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)f.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,.fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2x3ucvgo.4eb.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cfrruvyb.luy.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_svjneimu.gkz.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_svjneimu.gkz.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wqgzyu5l.f34.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\mozille.exe	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	567808
Entropy (8bit):	7.627302244469304
Encrypted:	false
SSDEEP:	12288:3v5+Ky22SH/s6TYnPEvvslosxkhoNB3Ps7hZJ:/029/enPEHkowNB/S
MD5:	9FD45110BAD75CDA6DE67232014AEB6E
SHA1:	A43016FA816AFD1693FB7F266DD032FD7F061C35
SHA-256:	B586CA95BA9557F7AD2434D01F96FF191B77541670894DF3B78AA3A8312AE092
SHA-512:	0B87028C9E9654BC3FC69797E9B241604C1A6266DF388E8E01CCE98F19507F5544B35AFD02462E2229D4F4C9B8D348AB9A0294B1802F98D6F80F608657BC7675
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a..... ....@.. ....@.....K.....T..... ....H.....text...4.... ....`.sdata.....@....rsrc...T..... .....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\tmp71CD.tmp	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.151412589996552
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtXxvn:cge4MYrFdOFzOzN33ODOiDdKrsuThv
MD5:	C286A082609C1C1A219FF01B51775164
SHA1:	F8A15ACBF3A55AD917F35566777A6EC4731DE800
SHA-256:	8ED2C4AF8E80335DE493A0A74226839E5505BA01BFD742C9A56A296878D9D636
SHA-512:	2FD055314D57E399D6CBB5FAFC7B98AD0910AD3D82F01A531C08EE36E8384FF1B86A6656741AE4C0E59E818EFFB92398BDF54ED7DADB7D0AA911982AA211A9E5
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpB8D1.tmp.bat	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	154
Entropy (8bit):	5.030771528412489
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViE2J5xAljkOAdLvmqRDWXp5cViE2J5xAlnTRINjio5Z6:hWKqTtT6WXp+N23fjdCvmq1WXp+N23fb
MD5:	07BDDF3468F5B8BEAFB3C3BFAA8E4C3D
SHA1:	92D16205F5D6F7B4CDFAD83119A5E47A8F430DB8
SHA-256:	7704F72B9FD7E75BDD3D3C8632B4F332120E94C1B8CAD84B6F62C2B63CEADD2C
SHA-512:	C10E87D75A658380DD96B9B7A94201C342BADEB4AE400B88CD21D72CBF76865307A1A5A645D6B36A9E4ECDB7FFADBAC212E97B4F0E5DE25C98B14B84AE0685C6
Malicious:	false
Reputation:	unknown
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Local\Temp\mozille.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmpB8D1.tmp.bat" /f /q..

C:\Users\user\AppData\Local\Temp\tmpCDE7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\mozille.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.151412589996552
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtXxvn:cge4MYrFdOFzOzN33ODOiDdKrsuThv
MD5:	C286A082609C1C1A219FF01B51775164
SHA1:	F8A15ACBF3A55AD917F35566777A6EC4731DE800
SHA-256:	8ED2C4AF8E80335DE493A0A74226839E5505BA01BFD742C9A56A296878D9D636
SHA-512:	2FD055314D57E399D6CBB5FAFC7B98AD0910AD3D82F01A531C08EE36E8384FF1B86A6656741AE4C0E59E818EFFB92398BDF54ED7DADB7D0AA911982AA211A9E5
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	567808
Entropy (8bit):	7.627302244469304
Encrypted:	false
SSDEEP:	12288:3v5+Ky22SH/s6TYnPEvvslosxkhoNB3Ps7hZJ:/029/enPEHkowNB/S
MD5:	9FD45110BAD75CDA6DE67232014AEB6E
SHA1:	A43016FA816AFD1693FB7F266DD032FD7F061C35
SHA-256:	B586CA95BA9557F7AD2434D01F96FF191B77541670894DF3B78AA3A8312AE092
SHA-512:	0B87028C9E9654BC3FC69797E9B241604C1A6266DF388E8E01CCE98F19507F5544B35AFD02462E2229D4F4C9B8D348AB9A0294B1802F98D6F80F608657BC7675
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a..... .....@.. ....@.....K.....T..... ....H.....text...4.... ....`.sdata.....@....rsrc...T..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV

C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe:Zone.Identifier	
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220112\PowerShell_transcript.138727.F_iUYR88.20220112090240.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5801
Entropy (8bit):	5.4133657955498915
Encrypted:	false
SSDEEP:	96:BZZhENMqDo1Z4ZUhENMqDo1ZsOI2jZohENMqDo1ZermmOZ1:c
MD5:	A60FA78FF988D57F3451E409235D01C5
SHA1:	ACE6418390C2687EC72117DD8A11F25FC9D830B2
SHA-256:	DC0A2EB75B913C1FD7C28E211C0045E678AC5D659706AFBF63967569CA69ED15
SHA-512:	7AACF764D22856EC2EB7773B26E7559A4DC20278BDE3BD689EE288956AA9A06A95886EE10DCF447C7CDB94396FE4C560C97E847BEE16D3B45C214236BE466CC7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220112090242..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe..Process ID: 5400..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220112090242..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe..**********..Windows PowerShell transcript start..Start time: 20220112090441..Username: computer\user..RunAs User: DESKTOP-716T77

C:\Users\user\Documents\20220112\PowerShell_transcript.138727.fhx+G1tL.20220112090212.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5801
Entropy (8bit):	5.41379343008454
Encrypted:	false
SSDEEP:	96:BZvhENVqDo1ZuZshENVqDo1ZEOI2jZPhENVqDo1ZnrmmOZ1:T
MD5:	5DB6DDA4F50FC48388AEB9886E8D92FA
SHA1:	1B375170354A7D83E1E9478A93C8A17ED180E735
SHA-256:	F26C8CA471D97986F5C2DC5DA82BBCA9DA4C4EAEBC5EFB88917BD5D88403A7ED
SHA-512:	0ABC022E484CC6A00878DDD0B92A7D445C930C5DE61085961CB9A30DDB1E4FDE2484294EF36252566E52AD2C5389185724F8EBEA476364255DB84D2BBBEDEEB
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220112090213..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe..Process ID: 6080..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220112090213..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe..**********..Windows PowerShell transcript start..Start time: 20220112090526..Username: computer\user..RunAs User: DESKTOP-716T77

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA

\Device\Null	
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AA4
Malicious:	false
Reputation:	unknown
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.627302244469304
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	RFQ_GGMC-Ref 12-01-2022.exe
File size:	567808
MD5:	9fd45110bad75cda6de67232014aeb6e
SHA1:	a43016fa816afd1693fb7f266dd032fd7f061c35
SHA256:	b586ca95ba9557f7ad2434d01f96ff191b77541670894df3b78aa3a8312ae092
SHA512:	0b87028c9e9654bc3fc69797e9b241604c1a6266df388e8e01cce98f19507f5544b35afd02462e2229d4f4c9b8d348ab9a0294b1802f98d6f80f608657bc7675
SSDEEP:	12288:3v5+Ky22SH/s6TYnPEvvslosxkhoNB3Ps7hZJ:/029/enPEHkowNB/S
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a..... ....@.. ....@.....

Static PE Info

General

Entrypoint:	0x48b82e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61DE32FE [Wed Jan 12 01:46:38 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x89834	0x89a00	False	0.843022678247	data	7.64899477975	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0x8c000	0x204	0x400	False	0.458984375	data	4.099059951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x554	0x600	False	0.340494791667	data	2.80510503091	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x90000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-09:02:52.180734	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	5512	49720	89.238.150.43	192.168.2.3
01/12/22-09:04:02.052703	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	5512	192.168.2.3	89.238.150.43
01/12/22-09:04:10.617296	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	5512	192.168.2.3	89.238.150.43

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RFQ_GGMC-Ref 12-01-2022.exe PID: 6964 Parent PID: 4648

General

Start time:	09:02:00

Start date:	12/01/2022
Path:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe"
Imagebase:	0x390000
File size:	567808 bytes
MD5 hash:	9FD45110BAD75CDA6DE67232014AEB6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.338424053.0000000002701000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.338424053.0000000002701000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6080 Parent PID: 6964

General

Start time:	09:02:10
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe
Imagebase:	0x50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6100 Parent PID: 6080

General

Start time:	09:02:11
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6136 Parent PID: 6964

General

Start time:	09:02:11
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lhWbLvHNlciwu" /XML "C:\Users\user\AppData\Local\Temp\tmp71CD.tmp
Imagebase:	0x1010000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5800 Parent PID: 6136

General

Start time:	09:02:13
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RFQ_GGMC-Ref 12-01-2022.exe PID: 7000 Parent PID: 6964

General

Start time:	09:02:13
Start date:	12/01/2022

Path:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
Imagebase:	0x160000
File size:	567808 bytes
MD5 hash:	9FD45110BAD75CDA6DE67232014AEB6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ_GGMC-Ref 12-01-2022.exe PID: 6948 Parent PID: 6964

General

Start time:	09:02:16
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ_GGMC-Ref 12-01-2022.exe
Imagebase:	0x580000
File size:	567808 bytes
MD5 hash:	9FD45110BAD75CDA6DE67232014AEB6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000000.335571895.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000000.335001041.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000002.359864523.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000000.334452217.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000000.333878908.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 5684 Parent PID: 6948

General

Start time:	09:02:29
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "mozille" /tr "'C:\Users\user\AppData\Local\Temp\mozille.exe'" & exit
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5852 Parent PID: 5684

General

Start time:	09:02:29
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 3868 Parent PID: 6948

General

Start time:	09:02:29
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmpB8D1.tmp.bat""
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 5580 Parent PID: 5684

General

Start time:	09:02:30
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "mozille" /tr "'C:\Users\user\AppData\Local\Temp\mozille.exe"'
Imagebase:	0x1010000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6276 Parent PID: 3868

General

Start time:	09:02:30
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 2292 Parent PID: 3868

General

Start time:	09:02:31
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x320000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mozille.exe PID: 6316 Parent PID: 664

General

Start time:	09:02:31
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Local\Temp\mozille.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\mozille.exe
Imagebase:	0x260000
File size:	567808 bytes
MD5 hash:	9FD45110BAD75CDA6DE67232014AEB6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.393670309.0000000002651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000002.393670309.0000000002651000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: mozille.exe PID: 6564 Parent PID: 3868

General

Start time:	09:02:36
Start date:	12/01/2022
Path:	C:\Users\user\AppData\Local\Temp\mozille.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\mozille.exe"
Imagebase:	0xf10000
File size:	567808 bytes
MD5 hash:	9FD45110BAD75CDA6DE67232014AEB6E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000F.00000002.572294732.00000000032C1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: 5400 Parent PID: 6316

General

Start time:	09:02:38
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe
Imagebase:	0x50000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5824 Parent PID: 5400

General

Start time:	09:02:39
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5192 Parent PID: 6316

General

Start time:	09:02:39
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lhWbLvHNlciwu" /XML "C:\Users\user\AppData\Local\Temp\tmpCDE7.tmp
Imagebase:	0x1010000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5452 Parent PID: 6564

General

Start time:	09:02:40
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lhWbLvHNlciwu.exe
Imagebase:	0x2d0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis