ID: 356280
Sample Name: OII9x4FeW7.exe
Cookbook: default.jbs
Time: 20:41:01
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

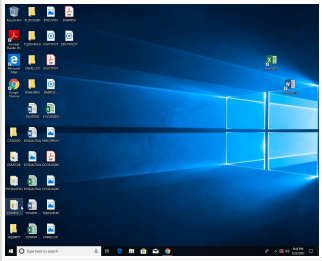
Analysis Report OII9x4FeW7.exe

Overview

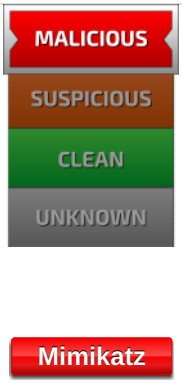
General Information

Sample Name:	OII9x4FeW7.exe
Analysis ID:	356280
MD5:	ff7d3b6003c9058..
SHA1:	842bbfb81f4a651..
SHA256:	c3304ec5296879..
Tags:	exe YoungLotus

Most interesting Screenshot:



Detection



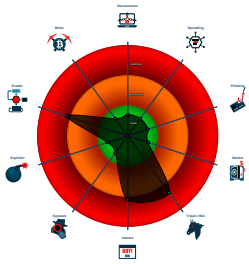
Mimikatz

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Mimikatz
- Drops PE files to the startup folder
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Sample is not signed and drops a de…
- Uses ping.exe to check the status o…
- Uses ping.exe to sleep
- AV process strings found (often use…

Classification



Startup

- **System is w10x64**
- OII9x4FeW7.exe (PID: 3604 cmdline: 'C:\Users\user\Desktop\OII9x4FeW7.exe' MD5: FF7D3B6003C9058E40AE38A6A7EFE40C)
  - Ogxog.exe (PID: 6188 cmdline: 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Ogxog.exe' MD5: FF7D3B6003C9058E40AE38A6A7EFE40C)
  - cmd.exe (PID: 6204 cmdline: C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C:\Users\user\Desktop\OII9X4~1.EXE > nul MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 6312 cmdline: ping -n 2 127.0.0.1 MD5: 70C24A306F768936563ABDADB9CA9108)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.514979015.000000001010 0000.00000004.00000001.sdmp	JoeSecurity_Mimikatz_1	Yara detected Mimikatz	Joe Security	
00000001.00000002.247680497.000000001010 0000.00000004.00000001.sdmp	JoeSecurity_Mimikatz_1	Yara detected Mimikatz	Joe Security	
Process Memory Space: OII9x4FeW7.exe PID: 3604	JoeSecurity_Mimikatz_1	Yara detected Mimikatz	Joe Security	
Process Memory Space: Ogxog.exe PID: 6188	JoeSecurity_Mimikatz_1	Yara detected Mimikatz	Joe Security	

Unpacked PEs

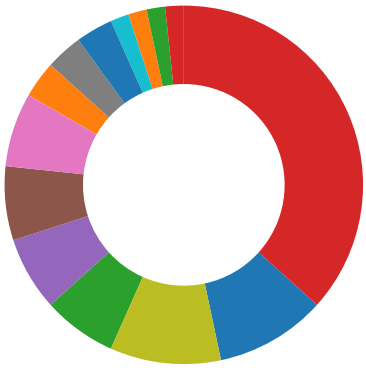
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
1.2.OII9x4FeW7.exe.10101928.5.raw.unpack	GhostDragon_Gh0stRAT	Detects Gh0st RAT mentioned in Cylance\' Ghost Dragon Report	Florian Roth	• 0x22ff0:$x4: Http/1.1 403 Forbidden • 0x22ff0:$s5: Http/1.1 403 Forbidden
1.2.OII9x4FeW7.exe.10101928.5.raw.unpack	Mimikatz_Strings	Detects Mimikatz strings	Florian Roth	• 0x22fa7:$x1: sekurlsa::logonpasswords
1.2.OII9x4FeW7.exe.10101928.5.raw.unpack	JoeSecurity_Mimikatz_1	Yara detected Mimikatz	Joe Security	
2.2.Ogxog.exe.10101928.4.raw.unpack	GhostDragon_Gh0stRAT	Detects Gh0st RAT mentioned in Cylance\' Ghost Dragon Report	Florian Roth	• 0x22ff0:$x4: Http/1.1 403 Forbidden • 0x22ff0:$s5: Http/1.1 403 Forbidden
2.2.Ogxog.exe.10101928.4.raw.unpack	Mimikatz_Strings	Detects Mimikatz strings	Florian Roth	• 0x22fa7:$x1: sekurlsa::logonpasswords
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Binary contains paths to debug symbols

Networking:

Uses ping.exe to check the status of other devices and networks

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample is not signed and drops a device driver

Boot Survival:

Drops PE files to the startup folder

Malware Analysis System Evasion:

Uses ping.exe to sleep

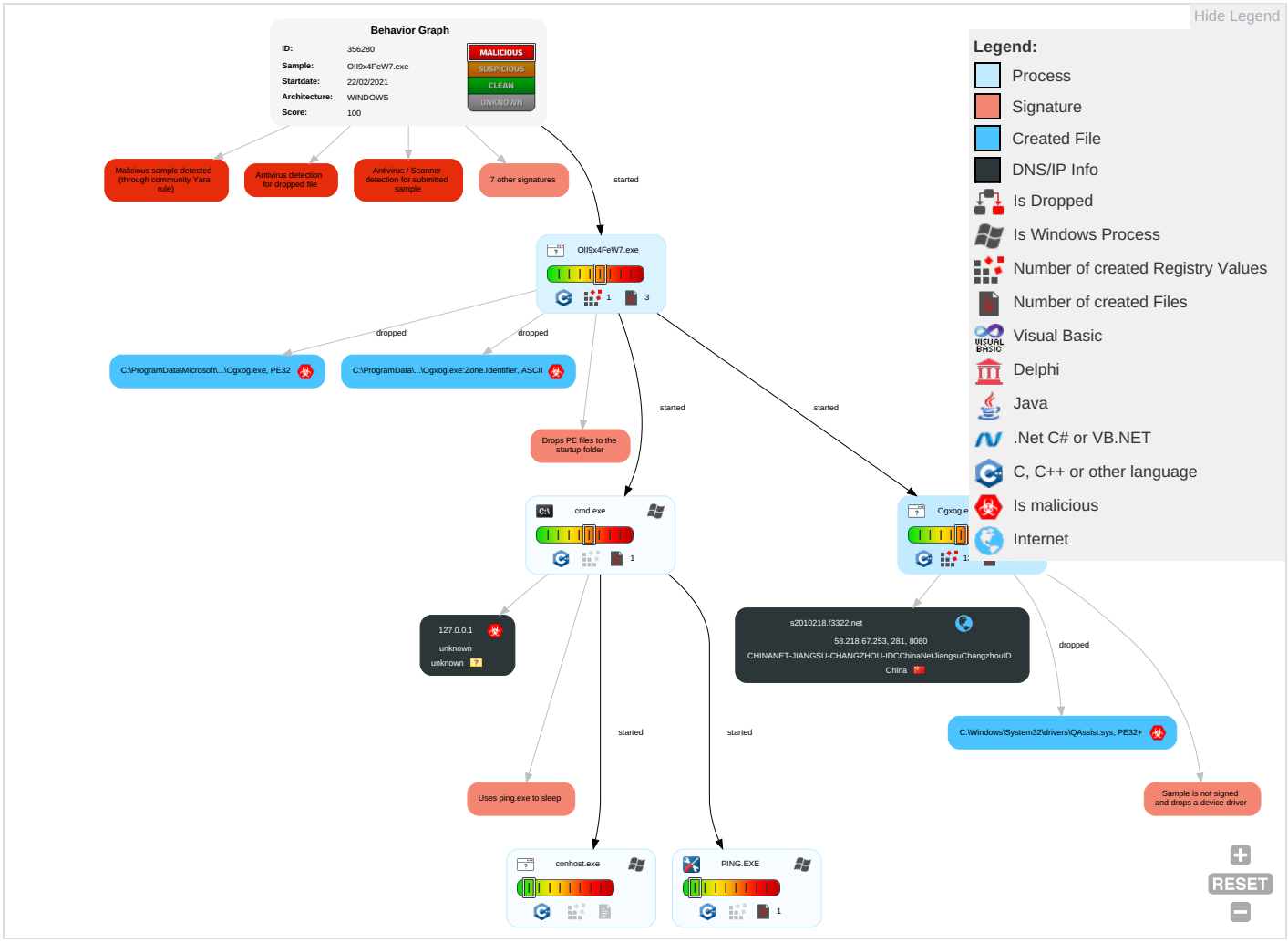
Stealing of Sensitive Information:

Yara detected Mimikatz

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	Native API 1	Startup Items 1	Startup Items 1	Masquerading 3	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communicatior
Default Accounts	Scheduled Task/Job	Windows Service 2	Windows Service 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1 2	Process Injection 1 2	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	LSASS Driver 2	Registry Run Keys / Startup Folder 1 2	Obfuscated Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	LSASS Driver 2	Software Packing	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station

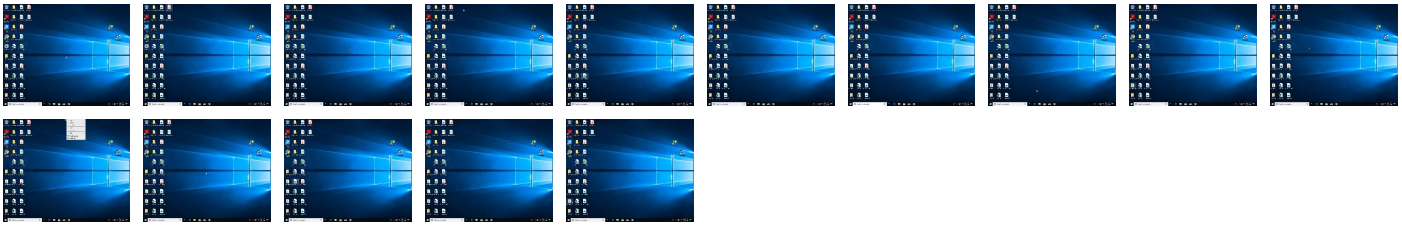
Behavior Graph



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
OII9x4FeW7.exe	73%	Virustotal		Browse
OII9x4FeW7.exe	77%	ReversingLabs	Win32.Backdoor.Farfli	
OII9x4FeW7.exe	100%	Avira	TR/Crypt.XPACK.Gen	
OII9x4FeW7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\System32\drivers\QAssist.sys	100%	Avira	RKIT/Agent.ccibt	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe	100%	Joe Sandbox ML		
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe	77%	ReversingLabs	Win32.Backdoor.Farfli	
C:\Windows\System32\drivers\QAssist.sys	47%	ReversingLabs	Win64.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.Ogxog.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.Ogxog.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.OII9x4FeW7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.OII9x4FeW7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://ssl.ptlogin2.qq.com%s	0%	Avira URL Cloud	safe	
http://ptlogin2.qun.qq.com%s	0%	Avira URL Cloud	safe	
http://qun.qq.com%s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s2010218.f3322.net	58.218.67.253	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ssl.ptlogin2.qq.com%s	OII9x4FeW7.exe, 00000001.00000002.247680497.0000000010100000.00000004.00000001.sdmp, Ogxog.exe, 00000002.00000002.514979015.0000000010100000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://xui.ptlogin2.qq.com/cgi-bin/xlogin?appid=715030901&daid=73&hide_close_icon=1&pt_no_auth=1&s_	OII9x4FeW7.exe, 00000001.00000002.247680497.0000000010100000.00000004.00000001.sdmp, Ogxog.exe, 00000002.00000002.514979015.0000000010100000.00000004.00000001.sdmp	false		high
http://ptlogin2.qun.qq.com%s	OII9x4FeW7.exe, 00000001.00000002.247680497.0000000010100000.00000004.00000001.sdmp, Ogxog.exe, 00000002.00000002.514979015.0000000010100000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://qun.qq.com%s	OII9x4FeW7.exe, 00000001.00000002.247680497.0000000010100000.00000004.00000001.sdmp, Ogxog.exe, 00000002.00000002.514979015.0000000010100000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
58.218.67.253	unknown	China		134769	CHINANET-JIANGSU-CHANGZHOU-IDCChinaNetJiangsuChangzhouID	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356280
Start date:	22.02.2021
Start time:	20:41:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OII9x4FeW7.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.evad.winEXE@8/4@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 70.5% (good quality ratio 64%) • Quality average: 78.7% • Quality standard deviation: 31.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 51.103.5.186, 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.104.144.132, 13.64.90.137, 40.88.32.150, 168.61.161.212, 184.30.24.56, 184.30.21.144, 51.103.5.159, 51.104.146.109, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • 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
20:41:59	API Interceptor	1096x Sleep call for process: Ogxog.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
58.218.67.253	mgZRDu7Jxu.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CHINANET-JIANGSU-CHANGZHOU-IDCChinaNetJiangsuChangzhouID	mgZRDu7Jxu.exe	Get hash	malicious	Browse	• 58.218.67.253

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Windows\System32\drivers\QAssist.sys	MoQCvCpfgw.exe	Get hash	malicious	Browse	
	dC5i7RPJtz.exe	Get hash	malicious	Browse	
	dTCaJ7tQjT.exe	Get hash	malicious	Browse	
	KrcT896PNT.exe	Get hash	malicious	Browse	
	egy7oSjGz0.dll	Get hash	malicious	Browse	
	dPTqTpDNrQ.exe	Get hash	malicious	Browse	
	qGMyccscIL.exe	Get hash	malicious	Browse	
	d6Ide0bYbh.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe

Process:	C:\Users\user\Desktop\OII9x4FeW7.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	409600
Entropy (8bit):	7.806057633930343
Encrypted:	false
SSDEEP:	6144:2SuxNOug5MI3KBau3EO8iZrEXA2czL6mWzdoZtAznpGuGEwJvfJ0s+VC:3ux9g5F6U2WOWczLygAzN6fJX
MD5:	FF7D3B6003C9058E40AE38A6A7EFE40C
SHA1:	842BBFB81F4A65112BC2D8E4AFF8B976E5DB9A55
SHA-256:	C3304EC52968793AE709CF7C7CAAD6ACAE0BDED8088F06CEFBEE55BDE0A9224F
SHA-512:	486865A075B6D87187EA73AE2E76A7537F8FD63A6743ADFBFC4225573E98187DE4C397771061E92442FB868AB48DF8CDE4B9E4EBBA2EF6D065456C8A4049EE9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 77%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...X,..X,..X,..S,..X,y.V,..X,..R,..X,y.,..X,..Y,..X,..i,..X,=.^,..X, ..\,..X,Rich..X,.....PE..L...0|.]..... .....<.....@..... .....`.....V.....E...\...(.... ...6..... .....data.....@....rsrc....6... ...8.....@..@..... ....

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\OII9x4FeW7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\QAssist.sys	
Process:	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	77896
Entropy (8bit):	6.14724588578885
Encrypted:	false
SSDEEP:	1536:svHIPCv5eT9OrLPC5VwHrhpTrkt5Ad53vE1qXn9Jm6Y:svHIPmn/rHrhpTrkt52E1qXpY
MD5:	4E34C068E764AD0FF0CB58BC4F143197
SHA1:	1A392A469FC8C65D80055C1A7AAEE27BF5EBE7C4
SHA-256:	6CCE28B275D5EC20992BB13790976CAF434AB46DDBFD5CFD431D33424943122B
SHA-512:	DCEA6D76452B1AC9E3C1FED7463FE873B4DD4603EC67A4E204C27BA2C1EA79415508C3044223626F0AE499A9B7A3D6FB283F0978B5E20A58E959C9440376E98
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 47%
Joe Sandbox View:	• Filename: MoQCvCpfgw.exe, Detection: malicious, Browse • Filename: dC5i7RPJtz.exe, Detection: malicious, Browse • Filename: dTCaJ7tQjT.exe, Detection: malicious, Browse • Filename: KrcT896PNT.exe, Detection: malicious, Browse • Filename: egy7oSjGz0.dll, Detection: malicious, Browse • Filename: dPTqTpDNrQ.exe, Detection: malicious, Browse • Filename: qGMyccscIL.exe, Detection: malicious, Browse • Filename: d6Ide0bYbh.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.\|\$./\$./\$./U\6/]$./U\ /]$./..{/X$./..x/]$./U\&/Y$./\$./.$./.U/V$./. k/]$./Rich\$./.....PE..d....E\.....".....@.....@.....`.....@..<.....0.....H....P..... ....text..... ..h.rdata.....@..H.data...0.... .....@....pdata.....0.....@..HINIT.....@..... ....b.reloc.....P.....@..B..... .....

\Device\Null	
Process:	C:\Windows\SysWOW64\PING.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	331
Entropy (8bit):	4.92149009030101
Encrypted:	false
SSDEEP:	6:PzLSLzMRfmWxHLThx2LThx0sW26VY7FwAFeMmvVOIHJFxMVlmJHaVFEG1vv:PKMRJpTeT0sBSAFSkIrxMVlmJHaVzvv
MD5:	2E512EE24AAB186D09E9A1F9B72A0569
SHA1:	C5BA2E0C0338FFEE13ED1FB6DA0CC9C000824B0B
SHA-256:	DB41050CA723A06D95B73FFBE40B32DE941F5EE474F129B2B33E91C67B72674F
SHA-512:	6B4487A088155E34FE5C642E1C3D46F63CB2DDD9E4092809CE6F3BEEFDEF0D1F8AA67F8E733EDE70B07F467ED5BB6F07104EEA4C1E7AC7E1A502A772F56F7D E9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..Pinging 127.0.0.1 with 32 bytes of data:..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128..Reply from 127.0.0.1: bytes=32 time<1ms TTL=128....Ping statistics for 127.0.0.1:.. Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),..Approximate round trip times in milli-seconds:.. Minimum = 0ms, Maximum = 0ms, Average = 0ms..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.806057633930343

General

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:	OII9x4FeW7.exe
File size:	409600
MD5:	ff7d3b6003c9058e40ae38a6a7efe40c
SHA1:	842bbfb81f4a65112bc2d8e4aff8b976e5db9a55
SHA256:	c3304ec52968793ae709cf7c7caad6acae0bded8088f06cefbee55bde0a9224f
SHA512:	486865a075b6d87187ea73ae2e76a7537f8fd63a6743adfbfc4225573e98187de4c397771061e92442fb868ab48df8cde4b9e4ebba2ef6d065456c8a4049ee98
SSDEEP:	6144:2SuxNOug5MI3KBau3EO8iZrEXA2czL6mWzdoZtAznpGuGEwJvfJ0s+VC:3ux9g5F6U2WOWczLygAzN6fJX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...X,..X,..X,..S,..X,y.V,..X,..R,..X,y..,..X,..Y,..X,..i,..X,=.^,..X,..\,..X,Rich..X,.....PE..L...0|.].....

File Icon

Icon Hash:	f0d2ec4ccce8d270

Static PE Info

General

Entrypoint:	0x45c790
Entrypoint Section:	.data
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5D977C30 [Fri Oct 4 17:06:56 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	19d4e66d725c89ba6712b82bebc8196d

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0045B568h
push 0045D560h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp

Instruction
call dword ptr [00401010h]
xor edx, edx
mov dl, ah
mov dword ptr [004606ACh], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [004606A8h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [004606A4h], ecx
shr eax, 10h
mov dword ptr [004606A0h], eax
push 00000001h
call 00007FBCC87D18FFh
pop ecx
test eax, eax
jne 00007FBCC87D0CEAh
push 0000001Ch
call 00007FBCC87D0DA8h
pop ecx
call 00007FBCC87D16AAh
test eax, eax
jne 00007FBCC87D0CEAh
push 00000010h
call 00007FBCC87D0D97h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007FBCC87D14D8h
call dword ptr [0040100Ch]
mov dword ptr [00460D58h], eax
call 00007FBCC87D1396h
mov dword ptr [00460690h], eax
call 00007FBCC87D113Fh
call 00007FBCC87D1081h
call 00007FBCC87D0D8Ch
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [00401008h]
call 00007FBCC87D1012h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007FBCC87D0CE8h
movzx eax, word ptr [ebp+00h]

Rich Headers

Programming Language:	• [C++] VS98 (6.0) SP6 build 8804 • [EXP] VC++ 6.0 SP5 build 8804 • [C] VS98 (6.0) SP6 build 8804 • [LNK] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x611d0	0x45	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60d5c	0x28	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x3690	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xc8	.data
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
.data	0x1000	0x60215	0x60400	False	0.923445109578	data	7.8782253441	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x3690	0x3800	False	0.337611607143	data	4.00280030121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x621e0	0xea8	data	Chinese	China
RT_ICON	0x63088	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	Chinese	China
RT_ICON	0x63930	0x568	GLS_BINARY_LSB_FIRST	Chinese	China
RT_ICON	0x63ec8	0x10a8	data	Chinese	China
RT_ICON	0x64f70	0x468	GLS_BINARY_LSB_FIRST	Chinese	China
RT_GROUP_ICON	0x63e98	0x30	data	Chinese	China
RT_GROUP_ICON	0x653d8	0x22	data	Chinese	China
RT_MANIFEST	0x65400	0x28b	XML 1.0 document text	Chinese	China

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, GetModuleHandleA, GetStartupInfoA, GetCommandLineA, GetVersion, ExitProcess, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, GetModuleFileNameA, FreeEnvironmentStringsA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, GetCurrentThreadId, TlsSetValue, TlsAlloc, SetLastError, TlsGetValue, GetLastError, GetEnvironmentVariableA, GetVersionExA, HeapDestroy, HeapCreate, VirtualFree, HeapFree, RtlUnwind, WriteFile, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetCPInfo, GetACP, GetOEMCP, HeapAlloc, VirtualAlloc, HeapReAlloc, LoadLibraryA, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, InterlockedDecrement, InterlockedIncrement

Exports

Name	Ordinal	Address
Loader	1	0x45c738

Possible Origin

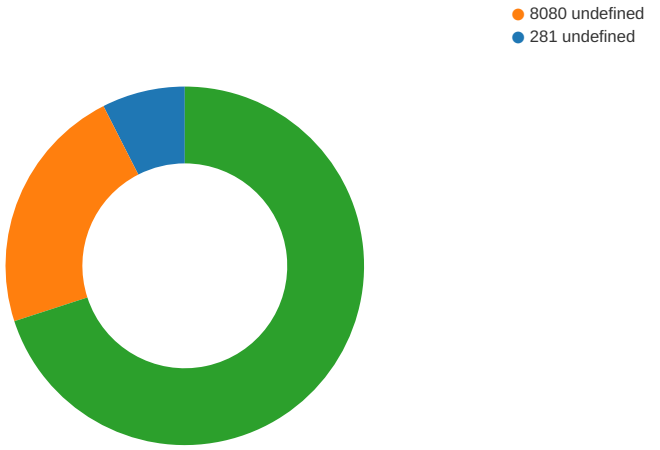
Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Network Port Distribution

Total Packets: 40

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:42:01.029640913 CET	49708	281	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:01.080394983 CET	49709	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:04.087625980 CET	49708	281	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:04.165674925 CET	49709	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:10.088187933 CET	49708	281	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:10.213155031 CET	49709	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:53.948281050 CET	49729	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:42:56.951469898 CET	49729	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:43:03.081592083 CET	49729	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:43:48.058778048 CET	49732	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:43:51.049793959 CET	49732	8080	192.168.2.5	58.218.67.253
Feb 22, 2021 20:43:57.065963984 CET	49732	8080	192.168.2.5	58.218.67.253

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:41:48.500123978 CET	52704	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:48.505867958 CET	52212	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:48.557265043 CET	53	52212	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:48.559782028 CET	53	52704	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:49.011498928 CET	54302	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:49.060205936 CET	53	54302	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:49.158063889 CET	53784	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:49.223365068 CET	53	53784	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:49.361866951 CET	65307	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:49.413301945 CET	53	65307	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:49.502137899 CET	64344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:49.550826073 CET	53	64344	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:51.354911089 CET	62060	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:51.403692961 CET	53	62060	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:52.531354904 CET	61805	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:52.580068111 CET	53	61805	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:53.553792953 CET	54795	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:53.602478981 CET	53	54795	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:54.484803915 CET	49557	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:54.542031050 CET	53	49557	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:55.732637882 CET	61733	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:55.784128904 CET	53	61733	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:57.307502031 CET	65447	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:57.358906984 CET	53	65447	8.8.8.8	192.168.2.5
Feb 22, 2021 20:41:58.987716913 CET	52441	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:41:59.036402941 CET	53	52441	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:00.254842997 CET	62176	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:00.304841042 CET	53	62176	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:00.736221075 CET	59596	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:42:01.060415983 CET	53	59596	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:01.588896036 CET	65296	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:01.642838001 CET	53	65296	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:02.764766932 CET	63183	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:02.813393116 CET	53	63183	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:04.300543070 CET	60151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:04.360558033 CET	53	60151	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:09.053586960 CET	56969	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:09.115528107 CET	53	56969	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:09.366693974 CET	55161	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:09.426685095 CET	53	55161	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:25.297349930 CET	54757	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:25.348947048 CET	53	54757	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:44.368484974 CET	49992	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:44.425599098 CET	53	49992	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:46.439716101 CET	60075	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:46.488514900 CET	53	60075	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:52.526004076 CET	55016	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:52.586776018 CET	53	55016	8.8.8.8	192.168.2.5
Feb 22, 2021 20:42:53.885593891 CET	64345	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:42:53.943073034 CET	53	64345	8.8.8.8	192.168.2.5
Feb 22, 2021 20:43:09.285339117 CET	57128	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:43:09.334151983 CET	53	57128	8.8.8.8	192.168.2.5
Feb 22, 2021 20:43:32.359483004 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:43:32.411156893 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 20:43:47.758420944 CET	50463	53	192.168.2.5	8.8.8.8
Feb 22, 2021 20:43:48.057722092 CET	53	50463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:42:00.736221075 CET	192.168.2.5	8.8.8.8	0x6780	Standard query (0)	s2010218.f3322.net	A (IP address)	IN (0x0001)
Feb 22, 2021 20:42:53.885593891 CET	192.168.2.5	8.8.8.8	0xc566	Standard query (0)	s2010218.f3322.net	A (IP address)	IN (0x0001)
Feb 22, 2021 20:43:47.758420944 CET	192.168.2.5	8.8.8.8	0x6914	Standard query (0)	s2010218.f3322.net	A (IP address)	IN (0x0001)

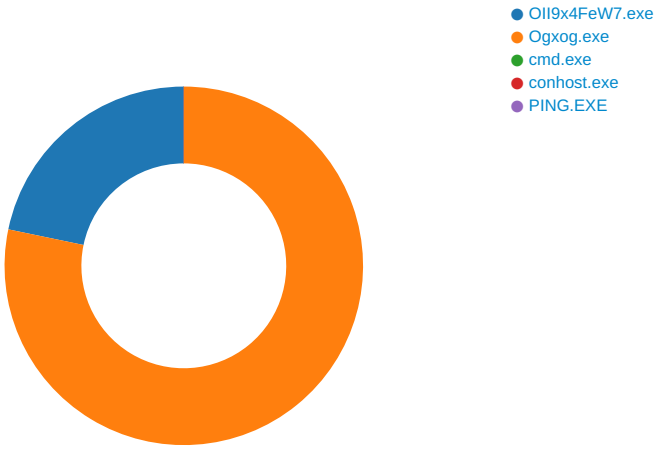
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:42:01.060415983 CET	8.8.8.8	192.168.2.5	0x6780	No error (0)	s2010218.f3322.net		58.218.67.253	A (IP address)	IN (0x0001)
Feb 22, 2021 20:42:53.943073034 CET	8.8.8.8	192.168.2.5	0xc566	No error (0)	s2010218.f3322.net		58.218.67.253	A (IP address)	IN (0x0001)
Feb 22, 2021 20:43:48.057722092 CET	8.8.8.8	192.168.2.5	0x6914	No error (0)	s2010218.f3322.net		58.218.67.253	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: OII9x4FeW7.exe PID: 3604 Parent PID: 5616

General

Start time:	20:41:58
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\OII9x4FeW7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OII9x4FeW7.exe'
Imagebase:	0x400000
File size:	409600 bytes
MD5 hash:	FF7D3B6003C9058E40AE38A6A7EFE40C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Mimikatz_1, Description: Yara detected Mimikatz, Source: 00000001.00000002.247680497.0000000010100000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
agmkis2	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1001A8F6	CopyFileA
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	1001A8F6	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 be ab 36 7f fa ca 58 2c fa ca 58 2c fa ca 58 2c cc ec 53 2c fb ca 58 2c 79 d6 56 2c ee ca 58 2c cc ec 52 2c c0 ca 58 2c 79 c2 05 2c f9 ca 58 2c fa ca 59 2c bb ca 58 2c ae e9 69 2c f8 ca 58 2c 3d cc 5e 2c fb ca 58 2c 05 ea 5c 2c fb ca 58 2c 52 69 63 68 fa ca 58 2c 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 30 7c 97 5d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........6...X,..X,..X,..S,.. X,y.V,..X,..R,..X,y..,..X,..Y, ..X,..i,..X,=.^,..X,..\,..X,Ri ch..X,........PE..L...0|.].....	success or wait	4	1001A8F6	CopyFileA
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	1001A8F6	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\Select	MarkTime	unicode	2021-02-22 20:41	success or wait	1	1000FF29	RegSetValueExA

Analysis Process: Ogxog.exe PID: 6188 Parent PID: 3604

General

Start time:	20:41:59
Start date:	22/02/2021
Path:	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Ogxog.exe
Wow64 process (32bit):	true
Commandline:	'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Ogxog.exe'
Imagebase:	0x400000
File size:	409600 bytes
MD5 hash:	FF7D3B6003C9058E40AE38A6A7EFE40C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Mimikatz_1, Description: Yara detected Mimikatz, Source: 00000002.00000002.514979015.0000000010100000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 77%, ReversingLabs

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\drivers\QAssist.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10015109	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\QAssist.sys	unknown	77896	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 18 45 db 7c 5c 24 b5 2f 5c 24 b5 2f 5c 24 b5 2f 55 5c 36 2f 5d 24 b5 2f 55 5c 20 2f 5d 24 b5 2f 81 db 7b 2f 58 24 b5 2f 81 db 78 2f 5d 24 b5 2f 55 5c 26 2f 59 24 b5 2f 5c 24 b4 2f 1c 24 b5 2f e9 ba 55 2f 56 24 b5 2f e9 ba 6b 2f 5d 24 b5 2f 52 69 63 68 5c 24 b5 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 e4 96 45 5c 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........E.\|\$./\$./\$./U\6/]$ ./U\ /]$./..{/X$./..x/]$./U\&/ Y$./\$./.$./..U/V$./..k/]$./Ri ch\$./....................... PE..d.....E\...	success or wait	1	10015140	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\QAssist	success or wait	1	100151BD	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\QAssist\Instances	success or wait	1	100155EA	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\QAssist\Instances\QAssist Instance	success or wait	1	10015765	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	Type	dword	2	success or wait	1	100151F3	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	Start	dword	1	success or wait	1	1001522E	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	ErrorControl	dword	0	success or wait	1	10015269	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	ImagePath	expand unicode	system32\DRIVERS\QAssist.sys	success or wait	1	10015302	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	DisplayName	unicode	QAssist	success or wait	1	1001533B	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	Group	unicode	FSFilter Activity Monitor	success or wait	1	1001538B	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	DependOnService	unicode array	FltMgr	success or wait	1	100153EE	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	DebugFlags	dword	0	success or wait	1	10015429	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	SupportedFeatures	dword	3	success or wait	1	10015464	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist	Hid_IgnoredImages	unicode array	\??\C:\Windows\system32\Services.exe;none	success or wait	1	10015527	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist\Instances	DefaultInstance	unicode	QAssist Instance	success or wait	1	10015658	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist\Instances\QAssist Instance	Altitude	unicode	370030	success or wait	1	100157AA	RegSetValueExA
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\QAssist\Instances\QAssist Instance	Flags	dword	0	success or wait	1	100157E5	RegSetValueExA

Analysis Process: cmd.exe PID: 6204 Parent PID: 3604

General

Start time:	20:41:59
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C:\Users\user\Desktop\OII9X4~1.EXE > nul
Imagebase:	0x330000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6268 Parent PID: 6204

General

Start time:	20:42:01
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: PING.EXE PID: 6312 Parent PID: 6204

General

Start time:	20:42:01
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping -n 2 127.0.0.1
Imagebase:	0xee0000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis