ID: 433012
Sample Name:
XQehPgTn35.exe
Cookbook: default.jbs
Time: 05:37:10
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

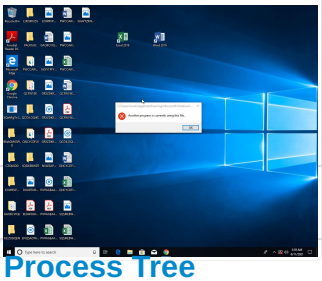
Analysis Report XQehPgTn35.exe

Overview

General Information

Sample Name:	XQehPgTn35.exe
Analysis ID:	433012
MD5:	595c00bf9ca4baa..
SHA1:	d1441cc336655f3..
SHA256:	6884ac9f82a44a7.
Tags:	exe njrat RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

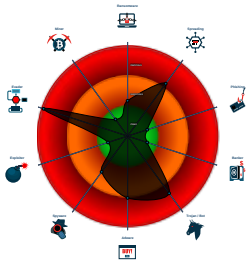
Njrat

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Njrat
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- XQehPgTn35.exe (PID: 6468 cmdline: 'C:\Users\user\Desktop\XQehPgTn35.exe' MD5: 595C00BF9CA4BAA42B4490F2782CF2D3)
  - server.exe (PID: 6616 cmdline: 'C:\Windows\server.exe' MD5: 595C00BF9CA4BAA42B4490F2782CF2D3)
    - netsh.exe (PID: 6700 cmdline: netsh firewall add allowedprogram 'C:\Windows\server.exe' 'server.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 6708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - netsh.exe (PID: 3544 cmdline: netsh firewall delete allowedprogram 'C:\Windows\server.exe' MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - netsh.exe (PID: 5700 cmdline: netsh firewall add allowedprogram 'C:\Windows\server.exe' 'server.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 1740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Microsoft Corporation.exe (PID: 5900 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe' MD5: 595C00BF9CA4BAA42B4490F2782CF2D3)
- Google.exe (PID: 6716 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe' MD5: 595C00BF9CA4BAA42B4490F2782CF2D3)
- **cleanup**

Malware Configuration

Threatname: Njrat


```
{
  "Campaign ID": "HacKed",
  "Version": "0.7d",
  "Install Name": "714bcaf02dc680243f761ccdcdc54f71",
  "Install Dir": "system 32",
  "Registry Value": "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
  "Host": "[i]",
  "Port": "MTU0MDkg",
  "Network Seprator": "714bcaf02dc680243f761ccdcdc54f71",
  "Mutex Name": "False",
  "BSOD Active": "MTU0MDkg",
  "Pastebin Link": "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
XQehPgTn35.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Google.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
C:\Program Files (x86)\Google.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
C:\SublimeText.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
C:\Program Files (x86)\Google.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
Click to see the 11 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.286063064.0000000001312000.00000040.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0000000E.00000002.286063064.0000000001312000.00000040.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x1585d:$reg: SEE_MASK_NOZONECHECKS • 0x154e3:$msg: Execute ERROR • 0x15537:$msg: Execute ERROR • 0x15aaf:$ping: cmd.exe /c ping 0 -n 2 & del
0000000B.00000002.254123068.0000000000DA2000.00000040.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0000000B.00000002.254123068.0000000000DA2000.00000040.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x1585d:$reg: SEE_MASK_NOZONECHECKS • 0x154e3:$msg: Execute ERROR • 0x15537:$msg: Execute ERROR • 0x15aaf:$ping: cmd.exe /c ping 0 -n 2 & del
00000000.00000002.201103366.0000000000AE2000.00000040.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.server.exe.9c0000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
11.0.Microsoft Corporation.exe.da0000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
0.0.XQehPgTn35.exe.ae0000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
14.0.Google.exe.1310000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x1162b1:$s1: zffb(==
0.2.XQehPgTn35.exe.ae0000.0.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Netsh Port or Application Allowed

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Njrat
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Detected unpacking (overwrites its own PE header)

Spreading:

- Contains functionality to spread to USB devices (.Net source)
- Creates autorun.inf (USB autostart)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Connects to many ports of the same IP (likely port scanning)

E-Banking Fraud:

- Yara detected Njrat

System Summary:

- Malicious sample detected (through community Yara rule)
- PE file has nameless sections

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker

Persistence and Installation Behavior:

- Drops PE files to the document folder of the user
- Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Drops PE files to the startup folder

Anti Debugging:

Hides threads from debuggers

Lowering of HIPS / PFW / Operating System Security Settings:

Disables the Windows task manager (taskmgr)

Modifies the windows firewall

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected Njrat

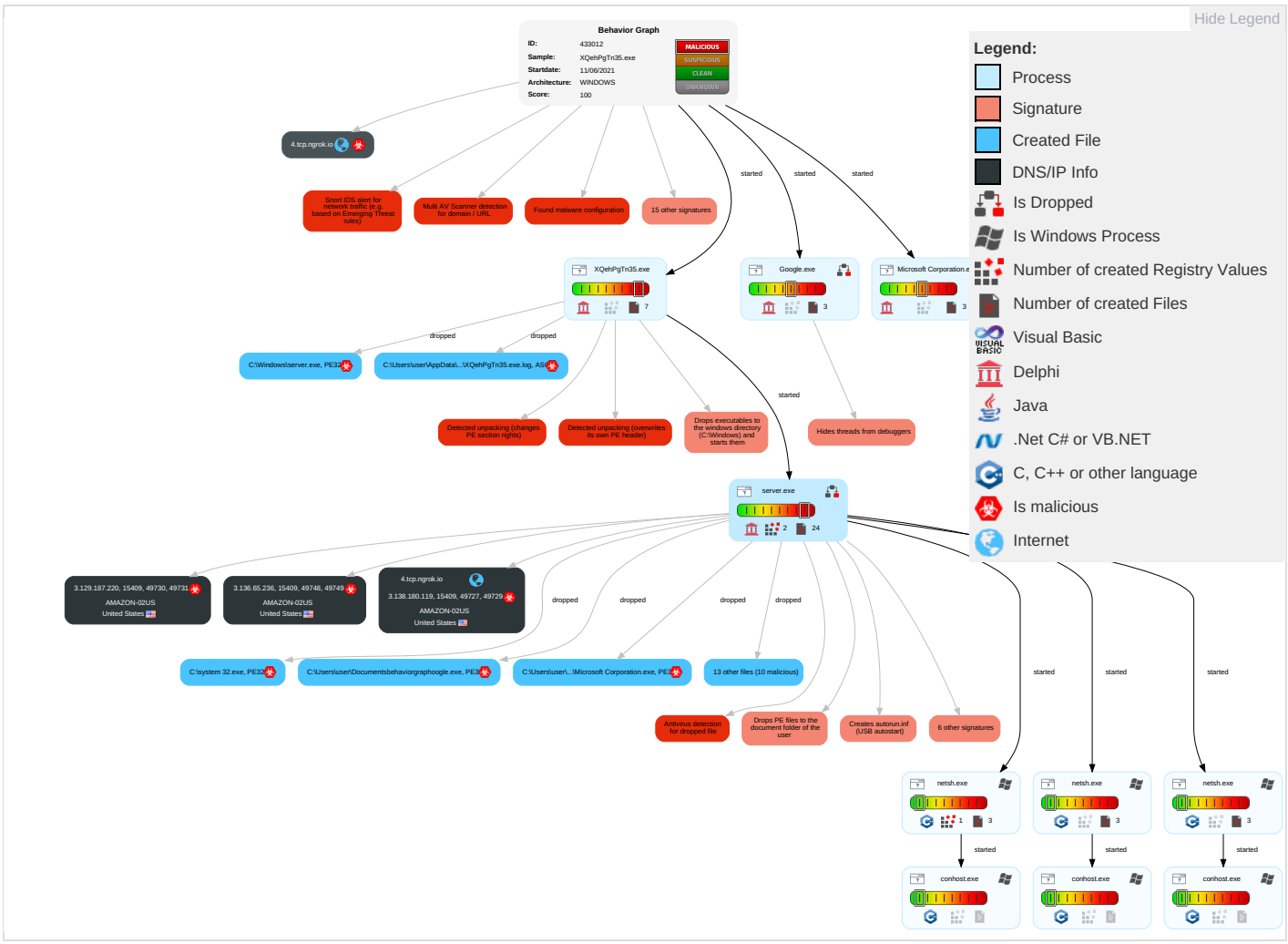
Remote Access Functionality:

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media 2 1	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Masquerading 1 3 2	Input Capture 1	Security Software Discovery 2 1 1	Replication Through Removable Media 2 1	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1 2	Process Injection 1 2	Disable or Modify Tools 3 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 2	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Devi 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	Application Layer Protocol 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Peripheral Device Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3 3	DCSync	File and Directory Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

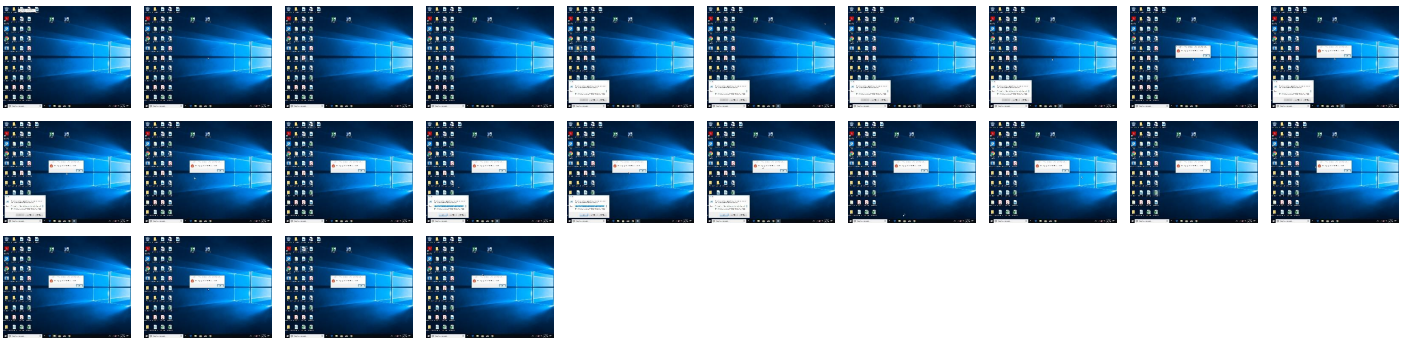
Behavior Graph



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
XQehPgTn35.exe	44%	Virustotal		Browse
XQehPgTn35.exe	43%	Metadefender		Browse
XQehPgTn35.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
XQehPgTn35.exe	100%	Avira	HEUR/AGEN.1128047	
XQehPgTn35.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Windows\server.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\system 32.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Umbrella.flv.exe	100%	Avira	HEUR/AGEN.1128047	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Avira	HEUR/AGEN.1128047	
C:\SublimeText.exe	100%	Avira	HEUR/AGEN.1128047	
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Windows\server.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\system 32.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Umbrella.flv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	100%	Joe Sandbox ML		
C:\SublimeText.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Google.exe	44%	Virustotal		Browse
C:\Program Files (x86)\Google.exe	43%	Metadefender		Browse
C:\Program Files (x86)\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\SublimeText.exe	43%	Metadefender		Browse
C:\SublimeText.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Umbrella.flv.exe	43%	Metadefender		Browse
C:\Umbrella.flv.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Google.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Microsoft\Windows\History\Google.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\History\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Google.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Google.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe	62%	ReversingLabs	Win32.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.Microsoft Corporation.exe.da0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.Google.exe.1310000.0.unpack	100%	Avira	HEUR/AGEN.1128047		Download File
0.2.XQehPgTn35.exe.afc000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
14.2.Google.exe.132c000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
14.2.Google.exe.1310000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.Microsoft Corporation.exe.dbc000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.server.exe.9c0000.0.unpack	100%	Avira	HEUR/AGEN.1128047		Download File
0.0.XQehPgTn35.exe.ae0000.0.unpack	100%	Avira	HEUR/AGEN.1128047		Download File
11.0.Microsoft Corporation.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1128047		Download File
0.2.XQehPgTn35.exe.ae0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
4.tcp.ngrok.io	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.enigmaprotector.com/	1%	Virustotal		Browse
http://www.enigmaprotector.com/	0%	Avira URL Cloud	safe	
[i]	0%	Avira URL Cloud	safe	
http://www.enigmaprotector.com/openU	1%	Virustotal		Browse
http://www.enigmaprotector.com/openU	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
4.tcp.ngrok.io	3.138.180.119	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
[i]	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.129.187.220	unknown	United States		16509	AMAZON-02US	true
3.138.180.119	4.tcp.ngrok.io	United States		16509	AMAZON-02US	true
3.136.65.236	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433012
Start date:	11.06.2021
Start time:	05:37:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XQehPgTn35.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:	24
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.spre.troj.adwa.evad.winEXE@14/27@35/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.6% (good quality ratio 7.4%) • Quality average: 74% • Quality standard deviation: 24.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:38:01	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe
05:38:12	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
05:38:25	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3.129.187.220	FiYBg9R8m0.exe	Get hash	malicious	Browse	
	BWAlL8lrQb.exe	Get hash	malicious	Browse	
	H4Q0l1RIuW.exe	Get hash	malicious	Browse	
	CpOFmSHBGH.exe	Get hash	malicious	Browse	
	GBtiwIB30h.exe	Get hash	malicious	Browse	
	63C2AB0ECE24B47CDCFE2128789214F87451A3D82D641.exe	Get hash	malicious	Browse	
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E678781.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCAAD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	J6wDHe2QdA.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	qiCot2DU55.exe	Get hash	malicious	Browse	
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	
	aYqoy7xF7y.exe	Get hash	malicious	Browse	
	Krtw4Kl87V.exe	Get hash	malicious	Browse	
	PsbfBdoToY.exe	Get hash	malicious	Browse	
	BcaDguoEzV.exe	Get hash	malicious	Browse	
	Oct Invoices 8984.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoices 489.exe	Get hash	malicious	Browse	
	Invoices 073.exe	Get hash	malicious	Browse	
3.138.180.119	BWAlL8lrQb.exe	Get hash	malicious	Browse	
	0BFE93ABC8B3801B7E906960F6D69CC51088B765 44EFC.exe	Get hash	malicious	Browse	
	ooAUh9ba7E.exe	Get hash	malicious	Browse	
	A6FAm1ae1j.exe	Get hash	malicious	Browse	
	GBtiwIB30h.exe	Get hash	malicious	Browse	
	vZvmgrCXam.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	J6wDHe2QdA.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	aYqoy7xF7y.exe	Get hash	malicious	Browse	
	Krtw4Kl87V.exe	Get hash	malicious	Browse	
	zOlLBCUG9R.exe	Get hash	malicious	Browse	
	ysJ2pAd54Z.exe	Get hash	malicious	Browse	
	rQMm2jZD.exe	Get hash	malicious	Browse	
	BcaDguoEzV.exe	Get hash	malicious	Browse	
3.136.65.236	H4Q0l1RIuW.exe	Get hash	malicious	Browse	
	ooAUh9ba7E.exe	Get hash	malicious	Browse	
	CpOFmSHBGH.exe	Get hash	malicious	Browse	
	GBtiwIB30h.exe	Get hash	malicious	Browse	
	63C2AB0ECE24B47CDCFE2128789214F87451A3D8 2D641.exe	Get hash	malicious	Browse	
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	
	tmkfdBpwAx.exe	Get hash	malicious	Browse	
	J6wDHe2QdA.exe	Get hash	malicious	Browse	
	LGKacQbjeH.exe	Get hash	malicious	Browse	
	qiCot2DU55.exe	Get hash	malicious	Browse	
	yEh8mVeLA6.exe	Get hash	malicious	Browse	
	XFdEhEAPeE.exe	Get hash	malicious	Browse	
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	
	aYqoy7xF7y.exe	Get hash	malicious	Browse	
	YFZX6dTsiT.exe	Get hash	malicious	Browse	
	rQMm2jZD.exe	Get hash	malicious	Browse	
	mNxVbma4uT.exe	Get hash	malicious	Browse	
	BcaDguoEzV.exe	Get hash	malicious	Browse	
	Invoices 485.exe	Get hash	malicious	Browse	
	Invoices 489.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
4.tcp.ngrok.io	FiYBg9R8m0.exe	Get hash	malicious	Browse	• 3.133.207.110
	BWAlL8lrQb.exe	Get hash	malicious	Browse	• 3.129.187.220
	0BFE93ABC8B3801B7E906960F6D69CC51088B765 44EFC.exe	Get hash	malicious	Browse	• 3.138.180.119
	H4Q0l1RIuW.exe	Get hash	malicious	Browse	• 3.129.187.220
	ooAUh9ba7E.exe	Get hash	malicious	Browse	• 3.133.207.110
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.133.207.110
	CpOFmSHBGH.exe	Get hash	malicious	Browse	• 3.133.207.110
	GBtiwIB30h.exe	Get hash	malicious	Browse	• 3.22.15.135
	vZvmgrCXam.exe	Get hash	malicious	Browse	• 3.138.180.119
	63C2AB0ECE24B47CDCFE2128789214F87451A3D8 2D641.exe	Get hash	malicious	Browse	• 3.136.65.236
	D3AAB88BB737961C971ED047B4C2D5B640EFF8E6 78781.exe	Get hash	malicious	Browse	• 3.22.15.135
	DC8DDCD4DB035FA647001A01CAB6A2866D092FCA AD182.exe	Get hash	malicious	Browse	• 3.129.187.220
	tmkfdBpwAx.exe	Get hash	malicious	Browse	• 3.131.147.49
	J6wDHe2QdA.exe	Get hash	malicious	Browse	• 3.136.65.236
	LGKacQbjeH.exe	Get hash	malicious	Browse	• 3.138.180.119
	qiCot2DU55.exe	Get hash	malicious	Browse	• 3.136.65.236

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yEh8mVeLA6.exe	Get hash	malicious	Browse	• 3.136.65.236
	XFdEhEAPeE.exe	Get hash	malicious	Browse	• 3.136.65.236
	YZJfsPAFBJ.exe	Get hash	malicious	Browse	• 3.131.147.49
	T91uHSVq.exe	Get hash	malicious	Browse	• 3.131.147.49

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	Docc.html	Get hash	malicious	Browse	• 13.224.99.74
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.209.246.140
	Sleek_Free.exe	Get hash	malicious	Browse	• 143.204.209.58
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.216.141.230
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 15.236.176.210
	WV Northern Community College.docx	Get hash	malicious	Browse	• 52.43.249.183
	wzdu53.exe	Get hash	malicious	Browse	• 13.249.13.113
	com.duolingo_1162_apps.evozi.com.apk	Get hash	malicious	Browse	• 52.222.174.5
AMAZON-02US	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	Docc.html	Get hash	malicious	Browse	• 13.224.99.74
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.209.246.140
	Sleek_Free.exe	Get hash	malicious	Browse	• 143.204.209.58
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.216.141.230
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 15.236.176.210
	WV Northern Community College.docx	Get hash	malicious	Browse	• 52.43.249.183
	wzdu53.exe	Get hash	malicious	Browse	• 13.249.13.113
	com.duolingo_1162_apps.evozi.com.apk	Get hash	malicious	Browse	• 52.222.174.5
AMAZON-02US	E1a92ARmPw.exe	Get hash	malicious	Browse	• 35.157.179.180
	crt9O3URua.exe	Get hash	malicious	Browse	• 35.157.179.180
	E1a92ARmPw.exe	Get hash	malicious	Browse	• 52.218.105.219
	DNPr7t0GMY.exe	Get hash	malicious	Browse	• 13.59.53.244
	ITAPQJikGw.exe	Get hash	malicious	Browse	• 99.83.154.118
	SKlGhwkzTi.exe	Get hash	malicious	Browse	• 44.227.65.245
	SecuriteInfo.com.Trojan.Packed2.43183.29557.exe	Get hash	malicious	Browse	• 13.59.53.244
	Letter 1019.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 143.204.98.37
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 75.2.26.18
	U03c2doc.exe	Get hash	malicious	Browse	• 108.128.23 8.226
	Letter 09JUN 2021.xlsx	Get hash	malicious	Browse	• 18.140.1.169
	Docc.html	Get hash	malicious	Browse	• 13.224.99.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.209.246.140
	Sleek_Free.exe	Get hash	malicious	Browse	• 143.204.209.58
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 52.216.141.230
	#Ud83d#Udcde_#U25b6#Ufe0f.htm	Get hash	malicious	Browse	• 15.236.176.210
	WV Northern Community College.docx	Get hash	malicious	Browse	• 52.43.249.183
	wzdu53.exe	Get hash	malicious	Browse	• 13.249.13.113
	com.duolingo_1162_apps.evozi.com.apk	Get hash	malicious	Browse	• 52.222.174.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\Google.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 44%, Browse • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L......`..................p............... ....@.. ....8......... ..@................................ .)..............................).. ....@............ ....@.............(............. ....@....data....@....)..,...F.............@..*FL.. ....

C:\SublimeText.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\SublimeText.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL.....

C:\Umbrella.flv.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Umbrella.flv.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL.....

C:\Users\user\AppData\Local\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Reputation:	low

C:\Users\user\AppData\Local\Google.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Google.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Microsoft Corporation.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\XQehPgTn35.exe.log	
Process:	C:\Users\user\Desktop\XQehPgTn35.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\History\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\History\Google.exe	
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe	
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\714bcaf02dc680243f761ccdcdc54f71Windows Updater.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....).....F.....@.....*FL..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVlg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....).....F.....@.....*FL..... .....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVlg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... .....@..... .....@.....(..... .....@....data....@....).....F.....@.....*FL..... .....

C:\Users\user\AppData\Roaming\app	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe
File Type:	UTF-8 Unicode (with BOM) text, with no line terminators
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:yn:yn

C:\Users\user\AppData\Roaming\app	
MD5:	24E9E7D7EEA4DE90C8FC67AE1145ABF2
SHA1:	DD9BB46CCC6340CA892CF17EBE32B9BDBADEE2D1
SHA-256:	BD6C1D15579254E8879ADA07376F93CB2E959F45670374892FDE2EFAF4194F6C
SHA-512:	5572AFD61C7BA666515A987F23AD0A05AB753BDC28CFA492ADB30200207427A4A38699D3B7981E0750414775A4CE72A209511951D38A8673C709B08774FCA01F
Malicious:	false
Preview:	.11

C:\Users\user\Desktop\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\Documents\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Users\user\Favorites\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

C:\Windows\SysWOW64\Google.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Windows\SysWOW64\Google.exe	
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL.....

C:\Windows\server.exe	
Process:	C:\Users\user\Desktop\XQehPgTn35.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Windows\server.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL.....

C:\autorun.inf	
Process:	C:\Windows\server.exe
File Type:	Microsoft Windows Autorun file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.474554204780528
Encrypted:	false
SSDEEP:	3:It1KV2PHQCyK0x:e1KAwCyD
MD5:	40B1630BE21F39CB17BD1963CAE5A207
SHA1:	63C14BD151D42820DD45C033363FA5B9E1D34124
SHA-256:	F87E55F1A423B65FD639146F71F6027DBD4D6E69B65D9A17F1744774AA6589E1
SHA-512:	833112ED4A9A3C621D2FFFC78F83502B2937B82A2CF9BC692D75D907CE2AA46C2D97CFE23C402DB3292B2DD2655FF8692C3CD00D5BA4D792C3D8AF24958E19 6
Malicious:	**true**
Preview:	[autorun]..open=C:\Umbrella.flv.exe..shellexecute=C:\..

C:\system 32.exe	
Process:	C:\Windows\server.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1143296
Entropy (8bit):	7.98927615016363
Encrypted:	false
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
MD5:	595C00BF9CA4BAA42B4490F2782CF2D3
SHA1:	D1441CC336655F36EFC3DB070F84701A1F68E51A
SHA-256:	6884AC9F82A44A7702C4807DEEC1640B66EB71F6C750DD0CA1D5D78632E626B5
SHA-512:	AAA673ADB4511D7E4BA5836F6874B047E8C2B31F86E005D46094A47626D23F97D72874307538C451541DBB44905503DF2227902E9F4CCFFA4D9836981ABCD2E6

C:\system 32.exe	
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\system 32.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8..... ..@..... .)..... ....@..... .....@.....(..... .....@....data....@....)..,...F.....@.....*FL..... .....

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	313
Entropy (8bit):	4.971939296804078
Encrypted:	false
SSDEEP:	6:/ojfKsUTGN8Ypox42k9L+DbGMKeQE+vigqAZs2E+AYeDPO+Yswyha:wjPIGNrkHk9iaeIM6ADDPOHyha
MD5:	689E2126A85BF55121488295EE068FA1
SHA1:	09BAAA253A49D80C18326DFBCA106551EBF22DD6
SHA-256:	D968A966EF474068E41256321F77807A042F1965744633D37A203A705662EC25
SHA-512:	C3736A8FC7E6573FA1B26FE6A901C05EE85C55A4A276F8F569D9EADC9A58BEC507D1BB90DBF9EA62AE79A6783178C69304187D6B90441D82E46F5F56172B5C5C
Malicious:	false
Preview:	..IMPORTANT: Command executed successfully...However, "netsh firewall" is deprecated;..use "netsh advfirewall firewall" instead...For more information on using "netsh advfirewall firewall" commands..instead of "netsh firewall", see KB article 947709..at https://go.microsoft.com/fwlink/?linkid=121488 .....Ok.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.98927615016363
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • 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:	XQehPgTn35.exe
File size:	1143296
MD5:	595c00bf9ca4baa42b4490f2782cf2d3
SHA1:	d1441cc336655f36efc3db070f84701a1f68e51a
SHA256:	6884ac9f82a44a7702c4807deec1640b66eb71f6c750dd0ca1d5d78632e626b5
SHA512:	aaa673adb4511d7e4ba5836f6874b047e8c2b31f86e005c46094a47626d23f97d72874307538c451541dbb44905503df2227902e9f4ccffa4d9836981abcd2e6
SSDEEP:	24576:DPnLbQ9A/PFjHhefsVJ1ff9IS/+AhMrRekPHnu6DNO:DPImPFUQJVIg+WMrwOu6DN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....p..... .....@.. .....8.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4087b0

General

Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x60B61FAE [Tue Jun 1 11:53:18 2021 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:	2e5467cba76f44a088d39f78c5e807b6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x2000	0x18000	0x8600	False	0.989884561567	data	7.97927562362	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1a000	0x2000	0x200	False	0.0546875	data	0.305313057312	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1c000	0x280000	0x2ba00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x29c000	0xe4000	0xe2c00	False	0.997420238423	data	7.9850157277	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-05:38:32.480901	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49727	15409	192.168.2.3	3.138.180.119
06/11/21-05:38:35.122490	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49729	15409	192.168.2.3	3.138.180.119
06/11/21-05:38:37.883521	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49730	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:40.816135	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49731	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:43.655370	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49732	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:46.534439	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49733	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:49.820340	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49734	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:52.550734	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49735	15409	192.168.2.3	3.129.187.220
06/11/21-05:38:55.325429	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49736	15409	192.168.2.3	3.138.180.119
06/11/21-05:38:58.026524	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49737	15409	192.168.2.3	3.129.187.220

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-05:39:01.781328	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49738	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:04.485435	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49739	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:08.299471	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49740	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:10.989140	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49741	15409	192.168.2.3	3.129.187.220
06/11/21-05:39:13.686687	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49742	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:16.472819	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49743	15409	192.168.2.3	3.129.187.220
06/11/21-05:39:19.192478	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49744	15409	192.168.2.3	3.129.187.220
06/11/21-05:39:21.879780	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49745	15409	192.168.2.3	3.129.187.220
06/11/21-05:39:26.277451	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49746	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:28.697781	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49747	15409	192.168.2.3	3.129.187.220
06/11/21-05:39:31.432722	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49748	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:34.209617	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49749	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:36.900868	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49750	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:39.620373	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49751	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:43.395380	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49752	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:46.772436	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49753	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:49.556360	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49754	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:52.263322	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49755	15409	192.168.2.3	3.136.65.236
06/11/21-05:39:54.965375	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49756	15409	192.168.2.3	3.138.180.119
06/11/21-05:39:57.721057	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49757	15409	192.168.2.3	3.136.65.236
06/11/21-05:40:00.642878	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49758	15409	192.168.2.3	3.136.65.236
06/11/21-05:40:03.342398	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49759	15409	192.168.2.3	3.138.180.119
06/11/21-05:40:06.076276	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49760	15409	192.168.2.3	3.138.180.119
06/11/21-05:40:08.799968	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49761	15409	192.168.2.3	3.138.180.119
06/11/21-05:40:11.612120	TCP	2021176	ET TROJAN Bladabindi/njRAT CnC Command (II)	49762	15409	192.168.2.3	3.138.180.119

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 05:38:28.096605062 CEST	192.168.2.3	8.8.8.8	0xf277	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:34.836051941 CEST	192.168.2.3	8.8.8.8	0xb8e8	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:37.599096060 CEST	192.168.2.3	8.8.8.8	0xee6	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:40.598186016 CEST	192.168.2.3	8.8.8.8	0x32c4	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 05:38:43.438324928 CEST	192.168.2.3	8.8.8.8	0x38f4	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:46.221971035 CEST	192.168.2.3	8.8.8.8	0xe038	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:49.135191917 CEST	192.168.2.3	8.8.8.8	0xd1a8	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:52.318876028 CEST	192.168.2.3	8.8.8.8	0xf5b5	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:55.058105946 CEST	192.168.2.3	8.8.8.8	0x8c7d	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:57.808234930 CEST	192.168.2.3	8.8.8.8	0x921b	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:01.317874908 CEST	192.168.2.3	8.8.8.8	0xb963	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:04.265638113 CEST	192.168.2.3	8.8.8.8	0x118b	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:07.983109951 CEST	192.168.2.3	8.8.8.8	0xfb61	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:10.783400059 CEST	192.168.2.3	8.8.8.8	0xf912	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:13.477179050 CEST	192.168.2.3	8.8.8.8	0xfec0	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:16.255187035 CEST	192.168.2.3	8.8.8.8	0x4d5a	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:18.974092960 CEST	192.168.2.3	8.8.8.8	0xbd57	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:21.679620981 CEST	192.168.2.3	8.8.8.8	0x8ed1	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:24.601767063 CEST	192.168.2.3	8.8.8.8	0x8f77	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:28.487149000 CEST	192.168.2.3	8.8.8.8	0x847c	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:31.214534998 CEST	192.168.2.3	8.8.8.8	0xbb5f	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:33.976038933 CEST	192.168.2.3	8.8.8.8	0x53ca	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:36.682391882 CEST	192.168.2.3	8.8.8.8	0x91f6	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:39.395881891 CEST	192.168.2.3	8.8.8.8	0x87b1	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:42.354665995 CEST	192.168.2.3	8.8.8.8	0x6eba	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:46.567203999 CEST	192.168.2.3	8.8.8.8	0x9a26	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:49.323838949 CEST	192.168.2.3	8.8.8.8	0x5276	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:52.042948008 CEST	192.168.2.3	8.8.8.8	0xd7a2	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:54.735972881 CEST	192.168.2.3	8.8.8.8	0x6e44	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:57.523766994 CEST	192.168.2.3	8.8.8.8	0xafac	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:00.395754099 CEST	192.168.2.3	8.8.8.8	0x659c	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:03.119240046 CEST	192.168.2.3	8.8.8.8	0x7d9e	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:05.865139008 CEST	192.168.2.3	8.8.8.8	0xacb3	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:08.588099957 CEST	192.168.2.3	8.8.8.8	0x593e	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:11.383903980 CEST	192.168.2.3	8.8.8.8	0xc299	Standard query (0)	4.tcp.ngrok.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:38:28.160732031 CEST	8.8.8.8	192.168.2.3	0xf277	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:34.896231890 CEST	8.8.8.8	192.168.2.3	0xb8e8	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:38:37.659429073 CEST	8.8.8.8	192.168.2.3	0xee6	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:40.660141945 CEST	8.8.8.8	192.168.2.3	0x32c4	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:43.497728109 CEST	8.8.8.8	192.168.2.3	0x38f4	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:46.285773993 CEST	8.8.8.8	192.168.2.3	0xe038	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:49.196597099 CEST	8.8.8.8	192.168.2.3	0xd1a8	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:52.380361080 CEST	8.8.8.8	192.168.2.3	0xf5b5	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:55.119384050 CEST	8.8.8.8	192.168.2.3	0x8c7d	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:38:57.862252951 CEST	8.8.8.8	192.168.2.3	0x921b	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:01.382457972 CEST	8.8.8.8	192.168.2.3	0xb963	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:04.324976921 CEST	8.8.8.8	192.168.2.3	0x118b	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:08.038408041 CEST	8.8.8.8	192.168.2.3	0xfb61	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:10.845694065 CEST	8.8.8.8	192.168.2.3	0xf912	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:13.538152933 CEST	8.8.8.8	192.168.2.3	0xfec0	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:16.316384077 CEST	8.8.8.8	192.168.2.3	0x4d5a	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:19.033886909 CEST	8.8.8.8	192.168.2.3	0xbd57	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:21.730010986 CEST	8.8.8.8	192.168.2.3	0x8ed1	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:24.661842108 CEST	8.8.8.8	192.168.2.3	0x8f77	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:28.546643972 CEST	8.8.8.8	192.168.2.3	0x847c	No error (0)	4.tcp.ngrok.io		3.129.187.220	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:31.275702953 CEST	8.8.8.8	192.168.2.3	0xbb5f	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:34.036474943 CEST	8.8.8.8	192.168.2.3	0x53ca	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:36.741065979 CEST	8.8.8.8	192.168.2.3	0x91f6	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:39.457341909 CEST	8.8.8.8	192.168.2.3	0x87b1	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:42.414808989 CEST	8.8.8.8	192.168.2.3	0x6eba	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:46.626611948 CEST	8.8.8.8	192.168.2.3	0x9a26	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:49.382500887 CEST	8.8.8.8	192.168.2.3	0x5276	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:52.093952894 CEST	8.8.8.8	192.168.2.3	0xd7a2	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 05:39:54.798815012 CEST	8.8.8.8	192.168.2.3	0x6e44	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:39:57.577550888 CEST	8.8.8.8	192.168.2.3	0xafac	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:00.449871063 CEST	8.8.8.8	192.168.2.3	0x659c	No error (0)	4.tcp.ngrok.io		3.136.65.236	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:03.181199074 CEST	8.8.8.8	192.168.2.3	0x7d9e	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:05.927911043 CEST	8.8.8.8	192.168.2.3	0xacb3	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:08.651952982 CEST	8.8.8.8	192.168.2.3	0x593e	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)
Jun 11, 2021 05:40:11.447014093 CEST	8.8.8.8	192.168.2.3	0xc299	No error (0)	4.tcp.ngrok.io		3.138.180.119	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: XQehPgTn35.exe PID: 6468 Parent PID: 5836

General

Start time:	05:37:55
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\XQehPgTn35.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\XQehPgTn35.exe'
Imagebase:	0xae0000
File size:	1143296 bytes
MD5 hash:	595C00BF9CA4BAA42B4490F2782CF2D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.201103366.0000000000AE2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.201103366.0000000000AE2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: server.exe PID: 6616 Parent PID: 6468

General

Start time:	05:37:57
Start date:	11/06/2021
Path:	C:\Windows\server.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\server.exe'
Imagebase:	0x9c0000
File size:	1143296 bytes
MD5 hash:	595C00BF9CA4BAA42B4490F2782CF2D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Windows\server.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: netsh.exe PID: 6700 Parent PID: 6616

General

Start time:	05:38:00
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram 'C:\Windows\server.exe' 'server.exe' ENABLE
Imagebase:	0xd90000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6708 Parent PID: 6700

General

Start time:	05:38:00
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: netsh.exe PID: 3544 Parent PID: 6616

General

Start time:	05:38:17
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall delete allowedprogram 'C:\Windows\server.exe'
Imagebase:	0xd90000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 6136 Parent PID: 3544

General

Start time:	05:38:18
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: netsh.exe PID: 5700 Parent PID: 6616

General

Start time:	05:38:18
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram 'C:\Windows\server.exe' 'server.exe' ENABLE
Imagebase:	0xd90000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 1740 Parent PID: 5700

General

Start time:	05:38:19
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: Microsoft Corporation.exe PID: 5900 Parent PID: 3388

General

Start time:	05:38:21
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe'
Imagebase:	0xda0000
File size:	1143296 bytes
MD5 hash:	595C00BF9CA4BAA42B4490F2782CF2D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000B.00000002.254123068.0000000000DA2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000B.00000002.254123068.0000000000DA2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Microsoft Corporation.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 62%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Google.exe PID: 6716 Parent PID: 3388

General

Start time:	05:38:34
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Google.exe'
Imagebase:	0x1310000
File size:	1143296 bytes
MD5 hash:	595C00BF9CA4BAA42B4490F2782CF2D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000E.00000002.286063064.0000000001312000.00000040.00020000.sdmp, Author: Joe Security • Rule: Njrat, Description: detect njRAT in memory, Source: 0000000E.00000002.286063064.0000000001312000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 43%, Metadefender, Browse • Detection: 62%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis