ID: 492550
Sample Name: E0QkjJowwG
Cookbook: default.jbs
Time: 20:03:17
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

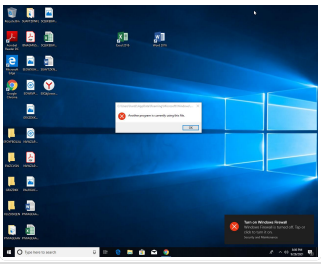
Windows Analysis Report E0QkjJowwG

Overview

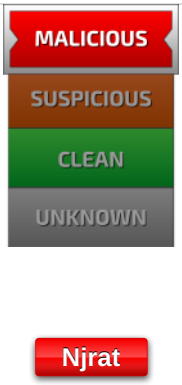
General Information

Sample Name:	E0QkjJowwG (renamed file extension from none to exe)
Analysis ID:	492550
MD5:	a1b69800aeb7ec..
SHA1:	96e25aed75903a..
SHA256:	09bc9c08f80f933..
Tags:	exe njrat
Infos:	

Most interesting Screenshot:



Detection



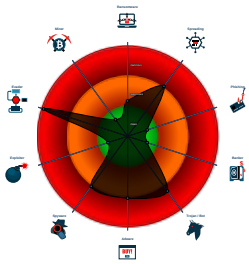
Njrat

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Hides threads from debuggers
- Uses netsh to modify the Windows n…
- Drops PE files to the startup folder
- Tries to evade analysis by execution…
- Connects to many ports of the same…
- .NET source code references suspic…
- Contains functionality to log keystro…

Classification



Process Tree

- **System is w10x64**
- E0QkjJowwG.exe (PID: 2700 cmdline: 'C:\Users\user\Desktop\E0QkjJowwG.exe' MD5: A1B69800AEB7ECBC49EBB13CE4A88737)
  - Yandex.exe (PID: 3100 cmdline: 'C:\Users\user\Yandex.exe' MD5: A1B69800AEB7ECBC49EBB13CE4A88737)
    - netsh.exe (PID: 4492 cmdline: netsh firewall add allowedprogram 'C:\Users\user\Yandex.exe' 'Yandex.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 4292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Yandex.exe (PID: 4420 cmdline: 'C:\Users\user\Yandex.exe' .. MD5: A1B69800AEB7ECBC49EBB13CE4A88737)
- Yandex.exe (PID: 4796 cmdline: 'C:\Users\user\Yandex.exe' .. MD5: A1B69800AEB7ECBC49EBB13CE4A88737)
- Yandex.exe (PID: 4764 cmdline: 'C:\Users\user\Yandex.exe' .. MD5: A1B69800AEB7ECBC49EBB13CE4A88737)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
E0QkjJowwG.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x45713:$s1: http:// • 0x4577d:$s1: http:// • 0x45b33:$s1: http:// • 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 • 0x45713:$f1: http:// • 0x4577d:$f1: http:// • 0x45b33:$f1: http://

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
C:\Users\user\Yandex.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	0x6dab:$a1: netsh firewall add allowedprogram 0x6d7b:$a2: SEE_MASK_NOZONECHECKS 0x6f9b:$b1: [TAP] 0x6e97:$c3: cmd.exe /c ping
00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	0x6d7b:$reg: SEE_MASK_NOZONECHECKS 0x6a6a:$msg: Execute ERROR 0x6ac2:$msg: Execute ERROR 0x6e97:$ping: cmd.exe /c ping 0 -n 2 & del
00000005.00000002.360786474.0000000000072000.00000040.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000005.00000002.360786474.0000000000072000.00000040.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	0x6dab:$a1: netsh firewall add allowedprogram 0x6d7b:$a2: SEE_MASK_NOZONECHECKS 0x6f9b:$b1: [TAP] 0x6e97:$c3: cmd.exe /c ping
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.Yandex.exe.70000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
5.0.Yandex.exe.70000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
0.0.E0QkjJowwG.exe.f20000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
6.0.Yandex.exe.70000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
7.0.Yandex.exe.70000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	0x45713:$s1: http:// 0x4577d:$s1: http:// 0x45b33:$s1: http:// 0x12f302:$s1: \xA4\xB8\xB8\xBC\xF6\xE3\xE3 0x45713:$f1: http:// 0x4577d:$f1: http:// 0x45b33:$f1: http://
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Netsh Port or Application Allowed

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Spreading:

Contains functionality to spread to USB devices (.Net source)

Networking:

Connects to many ports of the same IP (likely port scanning)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected Njrat

System Summary:

Malicious sample detected (through community Yara rule)

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Boot Survival:

- Drops PE files to the startup folder
- Creates autostart registry keys with suspicious names
- Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

- Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

- Tries to evade analysis by execution special instruction which cause usermode exception

Anti Debugging:

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings
- Modifies the windows firewall

Stealing of Sensitive Information:

- Yara detected Njrat

Remote Access Functionality:

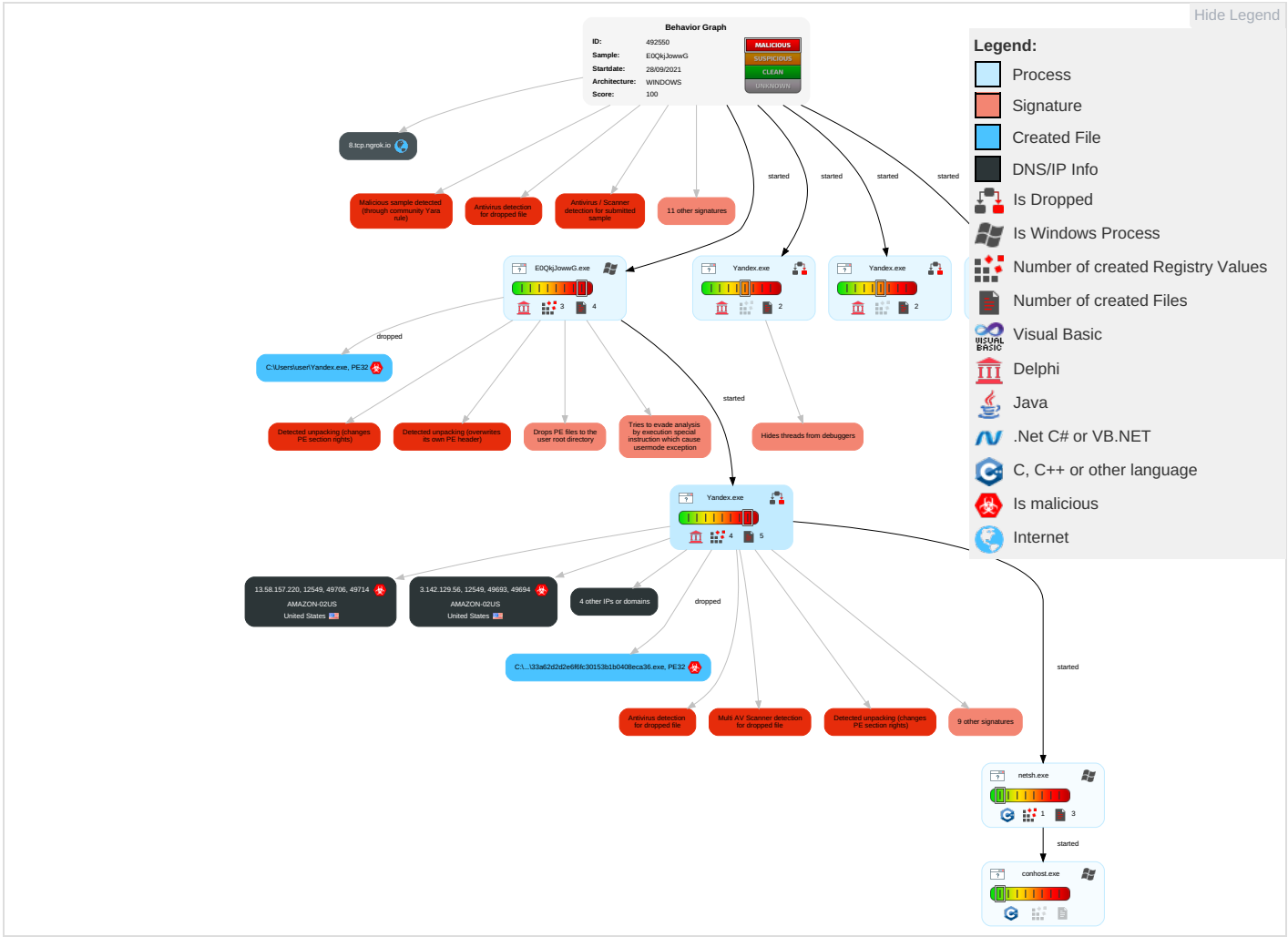
- Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Replication Through Removable Media 1 1	Native API 1	Startup Items 1	Startup Items 1	Masquerading 1 1 1	Input Capture 1 1	Security Software Discovery 3 1	Replication Through Removable Media 1 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 2 2 1	Process Injection 1 2	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 2 2 1	Disable or Modify Tools 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Explo Track Locat
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	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Peripheral Device Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

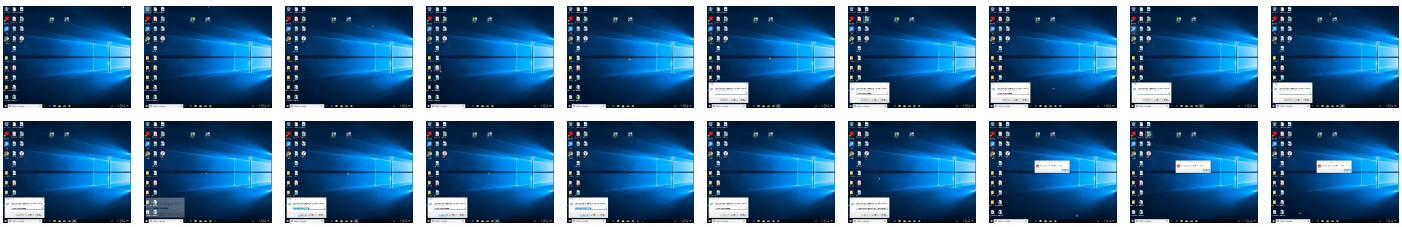
Behavior Graph

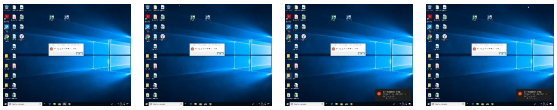


Screenshots

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
E0QkjJowwG.exe	43%	Virustotal		Browse
E0QkjJowwG.exe	34%	Metadefender		Browse
E0QkjJowwG.exe	60%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
E0QkjJowwG.exe	100%	Avira	HEUR/AGEN.1142875	
E0QkjJowwG.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	100%	Avira	HEUR/AGEN.1142875	
C:\Users\user\Yandex.exe	100%	Avira	HEUR/AGEN.1142875	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\Yandex.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	60%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\Yandex.exe	34%	Metadefender		Browse
C:\Users\user\Yandex.exe	60%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Yandex.exe.a0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
6.2.Yandex.exe.70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
1.2.Yandex.exe.70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.0.Yandex.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1142875		Download File
0.2.E0QkjJowwG.exe.f20000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
7.2.Yandex.exe.70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.2.Yandex.exe.70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.Yandex.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1142875		Download File
0.2.E0QkjJowwG.exe.f50000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.2.Yandex.exe.a0000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.Yandex.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1142875		Download File
7.0.Yandex.exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1142875		Download File
0.0.E0QkjJowwG.exe.f20000.0.unpack	100%	Avira	HEUR/AGEN.1142875		Download File
6.2.Yandex.exe.a0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
7.2.Yandex.exe.a0000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.enigmaprotector.com/	0%	URL Reputation	safe	
http://pki-ocsp.symauth.com0	0%	URL Reputation	safe	
http://www.enigmaprotector.com/openU	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
8.tcp.ngrok.io	3.19.130.43	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.142.129.56	unknown	United States		16509	AMAZON-02US	true
3.142.81.166	unknown	United States		16509	AMAZON-02US	true
3.142.167.4	unknown	United States		16509	AMAZON-02US	true
3.19.130.43	8.tcp.ngrok.io	United States		16509	AMAZON-02US	false
13.58.157.220	unknown	United States		16509	AMAZON-02US	true
3.142.167.54	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492550
Start date:	28.09.2021
Start time:	20:03:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	E0QkjJowwG (renamed file extension from none to 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:	12
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.spyw.evad.winEXE@9/3@32/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 88.1% (good quality ratio 83%) • Quality average: 77.9% • Quality standard deviation: 27.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:04:33	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 33a62d2d2e6f6fc30153b1b0408eca36 "C:\Users\user\Yandex.exe" ..
20:04:41	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 33a62d2d2e6f6fc30153b1b0408eca36 "C:\Users\user\Yandex.exe" ..
20:04:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 33a62d2d2e6f6fc30153b1b0408eca36 "C:\Users\user\Yandex.exe" ..
20:04:58	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe

Joe Sandbox View / Context

IPs

No context

Domains

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\33a62d2d2e6f6fc30153b1b0408eca36.exe	
Process:	C:\Users\user\Yandex.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246208
Entropy (8bit):	7.913768279846037
Encrypted:	false
SSDEEP:	24576:e5Cunz2U3pf2TDdQc1BSLppkpYTBFf4obQ4E7x12VludRAgxlJ:27f2TG+BSdpkqTBFpbVE7xYudOMl
MD5:	A1B69800AEB7ECBC49EBB13CE4A88737
SHA1:	96E25AED75903A5A84BE3175C6E834A44833BC5D
SHA-256:	09BC9C08F80F93317CD8769F85D8921787C677033A5B12A6C310FB92D83F6E41
SHA-512:	D4D5112B5F7C7ED676B2D41828B25A339A39235AAF8DE51BC1CFDD35A73ACF279CD3E7AC0434F93EAF20D35F9A5173FF0C49987B6D5B8E4E03131C29DEDC2C5
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\33a62d2d2e6f6fc30153b1b0408eca36.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....z.....:. .....@.. .....:. ..... .@... .. .. P,.....P,..... ...<... .....@..... .....\.....@..... .....^... .....@....rsrc.... .....`.....@.....)..... l.....@....data..... ,.....T.....@.....b0..J.6$.r..(.....

C:\Users\user\Yandex.exe	
Process:	C:\Users\user\Desktop\E0QkjJowwG.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246208
Entropy (8bit):	7.913768279846037
Encrypted:	false
SSDEEP:	24576:e5Cunz2U3pf2TDdQc1BSLppkpYTBFf4obQ4E7x12VludRAgxlJ:27f2TG+BSdpkqTBFpbVE7xYudOMl
MD5:	A1B69800AEB7ECBC49EBB13CE4A88737
SHA1:	96E25AED75903A5A84BE3175C6E834A44833BC5D
SHA-256:	09BC9C08F80F93317CD8769F85D8921787C677033A5B12A6C310FB92D83F6E41
SHA-512:	D4D5112B5F7C7ED676B2D41828B25A339A39235AAF8DE51BC1CFDD35A73ACF279CD3E7AC0434F93EAF20D35F9A5173FF0C49987B6D5B8E4E03131C29DEDC2C5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Users\user\Yandex.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	unknown

C:\Users\user\Yandex.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....z.....:. .....@.. .....:. ..... .@... .. .. P,.....P,..... ...<... .....@..... .....\.....@..... .....^... .....@....rsrc.... .....`.....@.....).....l.....@....data..... ,.....T.....@.....b0..J.6$.r..(..... .....

\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
Reputation:	unknown
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):	7.913768279846037
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:	E0QkjJowwG.exe
File size:	1246208
MD5:	a1b69800aeb7ecbc49ebb13ce4a88737
SHA1:	96e25aed75903a5a84be3175c6e834a44833bc5d
SHA256:	09bc9c08f80f93317cd8769f85d8921787c677033a5b12a6c310fb92d83f6e41
SHA512:	d4d5112b5f7c7ed676b2d41828b25a339a39235aaf8de51bc1cfdd35a73acf279cd3e7ac0434f93eaf20d35f9a5173ff0c49987b6d5b8e4e03131c29dedc20c5
SSDEEP:	24576:e5Cunz2U3pf2TDdQc1BSLppkpYTBFf4obQ4E7x12VludRAgxlJ:27f2TG+BSdpkqTBFpbVE7xYudOMl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....z.....:. .....@.. .....:. .....@... .. ..

File Icon

Icon Hash:	70c09286acceec31

Static PE Info

General

Entrypoint:	0x7ab9ec
Entrypoint Section:	.data
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x610909D1 [Tue Aug 3 09:18:09 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	0x8000	0x3c00	False	0.970572916667	data	7.92098871266	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0xa000	0x12000	0x200	False	0.072265625	data	0.487890975135	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1c000	0x2000	0x200	False	0.056640625	data	0.321716074313	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1e000	0x12000	0x10c00	False	0.185867537313	data	4.58721100046	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x30000	0x292000	0x2e800	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x2c2000	0xec000	0xeb000	False	0.987041846742	data	7.98017185611	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/28/21-20:04:32.486838	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60496	8.8.8.8	192.168.2.3
09/28/21-20:04:43.011013	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62151	8.8.8.8	192.168.2.3
09/28/21-20:04:50.439909	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49539	8.8.8.8	192.168.2.3
09/28/21-20:04:54.112899	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57558	8.8.8.8	192.168.2.3
09/28/21-20:05:11.955219	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58045	8.8.8.8	192.168.2.3
09/28/21-20:05:15.454923	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57459	8.8.8.8	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/28/21-20:05:22.686753	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
09/28/21-20:05:26.417990	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
09/28/21-20:05:58.855200	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52130	8.8.8.8	192.168.2.3
09/28/21-20:06:13.000628	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3
09/28/21-20:06:20.264329	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63297	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 20:04:32.464540958 CEST	192.168.2.3	8.8.8.8	0x453	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:35.990257978 CEST	192.168.2.3	8.8.8.8	0x97b8	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:39.490201950 CEST	192.168.2.3	8.8.8.8	0x1b5	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:42.990324020 CEST	192.168.2.3	8.8.8.8	0x18ea	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:46.492119074 CEST	192.168.2.3	8.8.8.8	0x5c16	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:50.417612076 CEST	192.168.2.3	8.8.8.8	0x9793	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:54.089463949 CEST	192.168.2.3	8.8.8.8	0x62d6	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:57.585732937 CEST	192.168.2.3	8.8.8.8	0x3b62	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:01.084588051 CEST	192.168.2.3	8.8.8.8	0xa907	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:04.733242989 CEST	192.168.2.3	8.8.8.8	0xd04a	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:08.423963070 CEST	192.168.2.3	8.8.8.8	0x1621	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:11.933850050 CEST	192.168.2.3	8.8.8.8	0x6106	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:15.433373928 CEST	192.168.2.3	8.8.8.8	0x62bd	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:18.929981947 CEST	192.168.2.3	8.8.8.8	0x813d	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:22.664371967 CEST	192.168.2.3	8.8.8.8	0xb69c	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:26.395843029 CEST	192.168.2.3	8.8.8.8	0xe838	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:29.904227972 CEST	192.168.2.3	8.8.8.8	0x3488	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:33.407552004 CEST	192.168.2.3	8.8.8.8	0x666b	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:36.903136969 CEST	192.168.2.3	8.8.8.8	0x9eca	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:40.521313906 CEST	192.168.2.3	8.8.8.8	0x7931	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:44.543060064 CEST	192.168.2.3	8.8.8.8	0xcb20	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:48.072393894 CEST	192.168.2.3	8.8.8.8	0x485	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:51.574587107 CEST	192.168.2.3	8.8.8.8	0x65ff	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:55.132102966 CEST	192.168.2.3	8.8.8.8	0x9d9f	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 20:05:58.832813025 CEST	192.168.2.3	8.8.8.8	0x3be7	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:02.340394020 CEST	192.168.2.3	8.8.8.8	0x9005	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:05.844444990 CEST	192.168.2.3	8.8.8.8	0x5888	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:09.352875948 CEST	192.168.2.3	8.8.8.8	0x1be3	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:12.970681906 CEST	192.168.2.3	8.8.8.8	0xd553	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:16.756254911 CEST	192.168.2.3	8.8.8.8	0xc9d8	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:20.244434118 CEST	192.168.2.3	8.8.8.8	0x611a	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:23.741792917 CEST	192.168.2.3	8.8.8.8	0xd1db	Standard query (0)	8.tcp.ngrok.io	A (IP address)	IN (0x0001)

DNS Answers

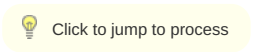
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 20:04:32.486838102 CEST	8.8.8.8	192.168.2.3	0x453	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:36.007617950 CEST	8.8.8.8	192.168.2.3	0x97b8	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:39.507852077 CEST	8.8.8.8	192.168.2.3	0x1b5	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:43.011013031 CEST	8.8.8.8	192.168.2.3	0x18ea	No error (0)	8.tcp.ngrok.io		3.142.129.56	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:46.511693001 CEST	8.8.8.8	192.168.2.3	0x5c16	No error (0)	8.tcp.ngrok.io		3.142.129.56	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:50.439908981 CEST	8.8.8.8	192.168.2.3	0x9793	No error (0)	8.tcp.ngrok.io		3.142.81.166	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:54.112899065 CEST	8.8.8.8	192.168.2.3	0x62d6	No error (0)	8.tcp.ngrok.io		3.142.167.4	A (IP address)	IN (0x0001)
Sep 28, 2021 20:04:57.604866028 CEST	8.8.8.8	192.168.2.3	0x3b62	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:01.102406979 CEST	8.8.8.8	192.168.2.3	0xa907	No error (0)	8.tcp.ngrok.io		3.142.167.4	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:04.751188993 CEST	8.8.8.8	192.168.2.3	0xd04a	No error (0)	8.tcp.ngrok.io		3.142.167.4	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:08.443677902 CEST	8.8.8.8	192.168.2.3	0x1621	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:11.955219030 CEST	8.8.8.8	192.168.2.3	0x6106	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:15.454922915 CEST	8.8.8.8	192.168.2.3	0x62bd	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:18.949404001 CEST	8.8.8.8	192.168.2.3	0x813d	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:22.686753035 CEST	8.8.8.8	192.168.2.3	0xb69c	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:26.417989969 CEST	8.8.8.8	192.168.2.3	0xe838	No error (0)	8.tcp.ngrok.io		13.58.157.220	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:29.924336910 CEST	8.8.8.8	192.168.2.3	0x3488	No error (0)	8.tcp.ngrok.io		3.142.167.4	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:33.427434921 CEST	8.8.8.8	192.168.2.3	0x666b	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:36.920691013 CEST	8.8.8.8	192.168.2.3	0x9eca	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 20:05:40.541754007 CEST	8.8.8.8	192.168.2.3	0x7931	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:44.562714100 CEST	8.8.8.8	192.168.2.3	0xcb20	No error (0)	8.tcp.ngrok.io		3.142.167.4	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:48.091933012 CEST	8.8.8.8	192.168.2.3	0x485	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:51.594619036 CEST	8.8.8.8	192.168.2.3	0x65ff	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:55.154114962 CEST	8.8.8.8	192.168.2.3	0x9d9f	No error (0)	8.tcp.ngrok.io		13.58.157.220	A (IP address)	IN (0x0001)
Sep 28, 2021 20:05:58.855200052 CEST	8.8.8.8	192.168.2.3	0x3be7	No error (0)	8.tcp.ngrok.io		3.142.167.54	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:02.361852884 CEST	8.8.8.8	192.168.2.3	0x9005	No error (0)	8.tcp.ngrok.io		3.142.167.54	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:05.864159107 CEST	8.8.8.8	192.168.2.3	0x5888	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:09.373269081 CEST	8.8.8.8	192.168.2.3	0x1be3	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:13.000627995 CEST	8.8.8.8	192.168.2.3	0xd553	No error (0)	8.tcp.ngrok.io		3.19.130.43	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:16.776082039 CEST	8.8.8.8	192.168.2.3	0xc9d8	No error (0)	8.tcp.ngrok.io		3.142.167.54	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:20.264328957 CEST	8.8.8.8	192.168.2.3	0x611a	No error (0)	8.tcp.ngrok.io		3.142.129.56	A (IP address)	IN (0x0001)
Sep 28, 2021 20:06:23.761253119 CEST	8.8.8.8	192.168.2.3	0xd1db	No error (0)	8.tcp.ngrok.io		3.142.167.54	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: E0QkjJowwG.exe PID: 2700 Parent PID: 4840

General

Start time:	20:04:14
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\E0QkjJowwG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\E0QkjJowwG.exe'
Imagebase:	0xf20000

File size:	1246208 bytes
MD5 hash:	A1B69800AEB7ECBC49EBB13CE4A88737
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.305336564.0000000000F22000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
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: Yandex.exe PID: 3100 Parent PID: 2700

General

Start time:	20:04:21
Start date:	28/09/2021
Path:	C:\Users\user\Yandex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Yandex.exe'
Imagebase:	0x70000
File size:	1246208 bytes
MD5 hash:	A1B69800AEB7ECBC49EBB13CE4A88737
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000001.00000002.558514473.0000000003CCE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000001.00000002.556263491.0000000000072000.00000040.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000001.00000002.556263491.0000000000072000.00000040.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000001.00000002.556263491.0000000000072000.00000040.00020000.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\Yandex.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 34%, Metadefender, Browse • Detection: 60%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: netsh.exe PID: 4492 Parent PID: 3100

General

Start time:	20:04:29
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram 'C:\Users\user\Yandex.exe' 'Yandex.exe' ENABLE
Imagebase:	0xe40000
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: 4292 Parent PID: 4492

General

Start time:	20:04:30
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Yandex.exe PID: 4420 Parent PID: 3352

General

Start time:	20:04:41

Start date:	28/09/2021
Path:	C:\Users\user\Yandex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Yandex.exe' ..
Imagebase:	0x70000
File size:	1246208 bytes
MD5 hash:	A1B69800AEB7ECBC49EBB13CE4A88737
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000005.00000002.360786474.0000000000072000.00000040.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000005.00000002.360786474.0000000000072000.00000040.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000005.00000002.360786474.0000000000072000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: Yandex.exe PID: 4796 Parent PID: 3352

General

Start time:	20:04:50
Start date:	28/09/2021
Path:	C:\Users\user\Yandex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Yandex.exe' ..
Imagebase:	0x70000
File size:	1246208 bytes
MD5 hash:	A1B69800AEB7ECBC49EBB13CE4A88737
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000006.00000002.378938056.0000000000072000.00000040.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000006.00000002.378938056.0000000000072000.00000040.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000006.00000002.378938056.0000000000072000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: Yandex.exe PID: 4764 Parent PID: 3352

General

Start time:	20:04:58
Start date:	28/09/2021
Path:	C:\Users\user\Yandex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Yandex.exe' ..
Imagebase:	0x70000
File size:	1246208 bytes
MD5 hash:	A1B69800AEB7ECBC49EBB13CE4A88737
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000007.00000002.396666249.0000000000072000.00000040.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000007.00000002.396666249.0000000000072000.00000040.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000007.00000002.396666249.0000000000072000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis