ID: 753416
Sample Name: itVg5XA6eK.exe
Cookbook: default.jbs
Time: 19:41:09
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

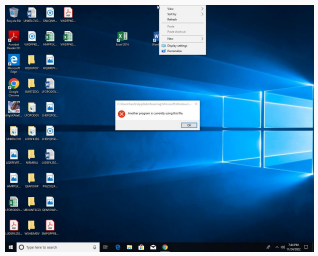
Windows Analysis Report

itVg5XA6eK.exe

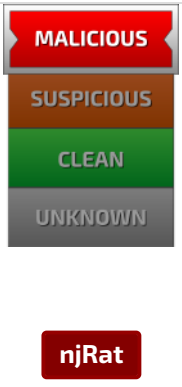
Overview

General Information

Sample Name:	itVg5XA6eK.exe
Analysis ID:	753416
MD5:	8533ef6f79e259e.
SHA1:	48c1f9b2a798a3..
SHA256:	bbc8cabc1ba4f8...
Tags:	exe njrat RAT
Infos:	



Detection



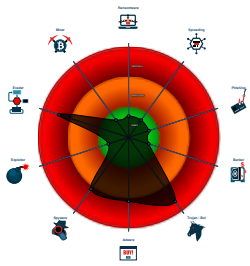
njRat

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

Signatures

- Multi AV Scanner detection for subm...
- Detected njRat
- Malicious sample detected (through...
- Yara detected Njrat
- Antivirus / Scanner detection for sub...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop...
- Snort IDS alert for network traffic
- Uses netsh to modify the Windows ...
- Drops PE files to the startup folder

Classification



Process Tree

- **System is w10x64**
- itVg5XA6eK.exe (PID: 6104 cmdline: C:\Users\user\Desktop\itVg5XA6eK.exe MD5: 8533EF6F79E259E9E5FE7C28F1FCD372)
  - rejdit_free_fire.exe (PID: 1852 cmdline: "C:\ProgramData\rejdit_free_fire.exe" MD5: 8533EF6F79E259E9E5FE7C28F1FCD372)
    - netsh.exe (PID: 2436 cmdline: netsh firewall add allowedprogram "C:\ProgramData\rejdit_free_fire.exe" "rejdit_free_fire.exe" ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- rejdit_free_fire.exe (PID: 644 cmdline: "C:\ProgramData\rejdit_free_fire.exe" .. MD5: 8533EF6F79E259E9E5FE7C28F1FCD372)
- rejdit_free_fire.exe (PID: 1280 cmdline: "C:\ProgramData\rejdit_free_fire.exe" .. MD5: 8533EF6F79E259E9E5FE7C28F1FCD372)
- rejdit_free_fire.exe (PID: 1112 cmdline: "C:\ProgramData\rejdit_free_fire.exe" .. MD5: 8533EF6F79E259E9E5FE7C28F1FCD372)
- **cleanup**

Malware Configuration

Threatname: Njrat

```
{
  "Host": "h43vipforyou.ddns.net",
  "Port": "1177",
  "Version": "0.7d",
  "Campaign ID": "HacKed",
  "Install Name": "rejdit_free_fire.exe",
  "Install Dir": "AllUsersProfile",
  "Network Seprator": "|'|'|"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
itVg5XA6eK.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
itVg5XA6eK.exe	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x4ce8:$s1: netsh firewall delete allowedprogram • 0x4dc4:$s2: netsh firewall add allowedprogram • 0x4d56:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x4e6c:$s4: Execute ERROR • 0x4ec8:$s4: Execute ERROR • 0x4e90:$s5: Download ERROR • 0x4ff4:$s6: [kl]
itVg5XA6eK.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4dc4:$a1: netsh firewall add allowedprogram • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x503e:$b1: [TAP] • 0x4d56:$c3: cmd.exe /c ping
itVg5XA6eK.exe	Windows_Trojan_Njrat_30f3c220	unknown	unknown	• 0x3c9a:$a1: get_Registry • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x4e90:$a3: Download ERROR • 0x4d56:$a4: cmd.exe /c ping 0 -n 2 & del " • 0x4ce8:$a5: netsh firewall delete allowedprogram "
itVg5XA6eK.exe	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d94:$reg: SEE_MASK_NOZONECHECKS • 0x4e6c:$msg: Execute ERROR • 0x4ec8:$msg: Execute ERROR • 0x4d56:$ping: cmd.exe /c ping 0 -n 2 & del

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\rejdit_free_fire.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
C:\ProgramData\rejdit_free_fire.exe	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x4ce8:$s1: netsh firewall delete allowedprogram • 0x4dc4:$s2: netsh firewall add allowedprogram • 0x4d56:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x4e6c:$s4: Execute ERROR • 0x4ec8:$s4: Execute ERROR • 0x4e90:$s5: Download ERROR • 0x4ff4:$s6: [kl]
C:\ProgramData\rejdit_free_fire.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4dc4:$a1: netsh firewall add allowedprogram • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x503e:$b1: [TAP] • 0x4d56:$c3: cmd.exe /c ping
C:\ProgramData\rejdit_free_fire.exe	Windows_Trojan_Njrat_30f3c220	unknown	unknown	• 0x3c9a:$a1: get_Registry • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x4e90:$a3: Download ERROR • 0x4d56:$a4: cmd.exe /c ping 0 -n 2 & del " • 0x4ce8:$a5: netsh firewall delete allowedprogram "
C:\ProgramData\rejdit_free_fire.exe	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d94:$reg: SEE_MASK_NOZONECHECKS • 0x4e6c:$msg: Execute ERROR • 0x4ec8:$msg: Execute ERROR • 0x4d56:$ping: cmd.exe /c ping 0 -n 2 & del

Click to see the 5 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x7bb4:$a1: netsh firewall add allowedprogram • 0x7b84:$a2: SEE_MASK_NOZONECHECKS • 0x7e2e:$b1: [TAP] • 0x7b46:$c3: cmd.exe /c ping
00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Njrat_30f3c220	unknown	unknown	• 0x6a8a:$a1: get_Registry • 0x7b84:$a2: SEE_MASK_NOZONECHECKS • 0x7c80:$a3: Download ERROR • 0x7b46:$a4: cmd.exe /c ping 0 -n 2 & del " • 0x7ad8:$a5: netsh firewall delete allowedprogram "
00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x7b84:$reg: SEE_MASK_NOZONECHECKS • 0x7c5c:$msg: Execute ERROR • 0x7cb8:$msg: Execute ERROR • 0x7b46:$ping: cmd.exe /c ping 0 -n 2 & del
00000000.00000000.239853870.0000000000442000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.itVg5XA6eK.exe.3ab6df0.0.raw.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0.2.itVg5XA6eK.exe.3ab6df0.0.raw.unpack	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x4ce8:$s1: netsh firewall delete allowedprogram • 0x4dc4:$s2: netsh firewall add allowedprogram • 0x4d56:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x4e6c:$s4: Execute ERROR • 0x4ec8:$s4: Execute ERROR • 0x4e90:$s5: Download ERROR • 0x4ff4:$s6: [kl]
0.2.itVg5XA6eK.exe.3ab6df0.0.raw.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4dc4:$a1: netsh firewall add allowedprogram • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x503e:$b1: [TAP] • 0x4d56:$c3: cmd.exe /c ping
0.2.itVg5XA6eK.exe.3ab6df0.0.raw.unpack	Windows_Trojan_Njrat_30f3c220	unknown	unknown	• 0x3c9a:$a1: get_Registry • 0x4d94:$a2: SEE_MASK_NOZONECHECKS • 0x4e90:$a3: Download ERROR • 0x4d56:$a4: cmd.exe /c ping 0 -n 2 & del " • 0x4ce8:$a5: netsh firewall delete allowedprogram "
0.2.itVg5XA6eK.exe.3ab6df0.0.raw.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d94:$reg: SEE_MASK_NOZONECHECKS • 0x4e6c:$msg: Execute ERROR • 0x4ec8:$msg: Execute ERROR • 0x4d56:$ping: cmd.exe /c ping 0 -n 2 & del
Click to see the 10 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394969911772033132 11/24/22-19:42:23.177340
SID:	2033132
Source Port:	49699
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394969911772825563 11/24/22-19:42:23.319941
SID:	2825563
Source Port:	49699
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970111772825563 11/24/22-19:43:29.909277
SID:	2825563
Source Port:	49701
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970011772033132 11/24/22-19:42:56.789376
SID:	2033132
Source Port:	49700
Destination Port:	1177

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394969911772825564 11/24/22-19:42:28.743067
SID:	2825564
Source Port:	49699
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970011772825564 11/24/22-19:43:01.745518
SID:	2825564
Source Port:	49700
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970011772825563 11/24/22-19:42:56.884058
SID:	2825563
Source Port:	49700
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970111772033132 11/24/22-19:43:29.805466
SID:	2033132
Source Port:	49701
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970111772814856 11/24/22-19:43:29.909277
SID:	2814856
Source Port:	49701
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970211772825563 11/24/22-19:44:02.683537
SID:	2825563
Source Port:	49702
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njRAT/Bladabindi CnC Callback (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239	
Timestamp:	192.168.2.341.109.68.2394970111772814860 11/24/22-19:43:44.045655
SID:	2814860
Source Port:	49701
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970211772033132 11/24/22-19:44:02.583206
SID:	2033132
Source Port:	49702
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njRAT/Bladabindi CnC Callback (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394969911772814860 11/24/22-19:42:28.743067
SID:	2814860
Source Port:	49699
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970211772814856 11/24/22-19:44:02.683537
SID:	2814856
Source Port:	49702
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njRAT/Bladabindi CnC Callback (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970011772814860 11/24/22-19:43:01.745518
SID:	2814860
Source Port:	49700
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970111772825564 11/24/22-19:43:44.045655
SID:	2825564
Source Port:	49701
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394970011772814856 11/24/22-19:42:56.884058
SID:	2814856
Source Port:	49700
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf) - Source IP: 192.168.2.3 - Destination IP: 41.109.68.239

Timestamp:	192.168.2.341.109.68.2394969911772814856 11/24/22-19:42:23.319941
SID:	2814856
Source Port:	49699
Destination Port:	1177
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud

Yara detected Njrat

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

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

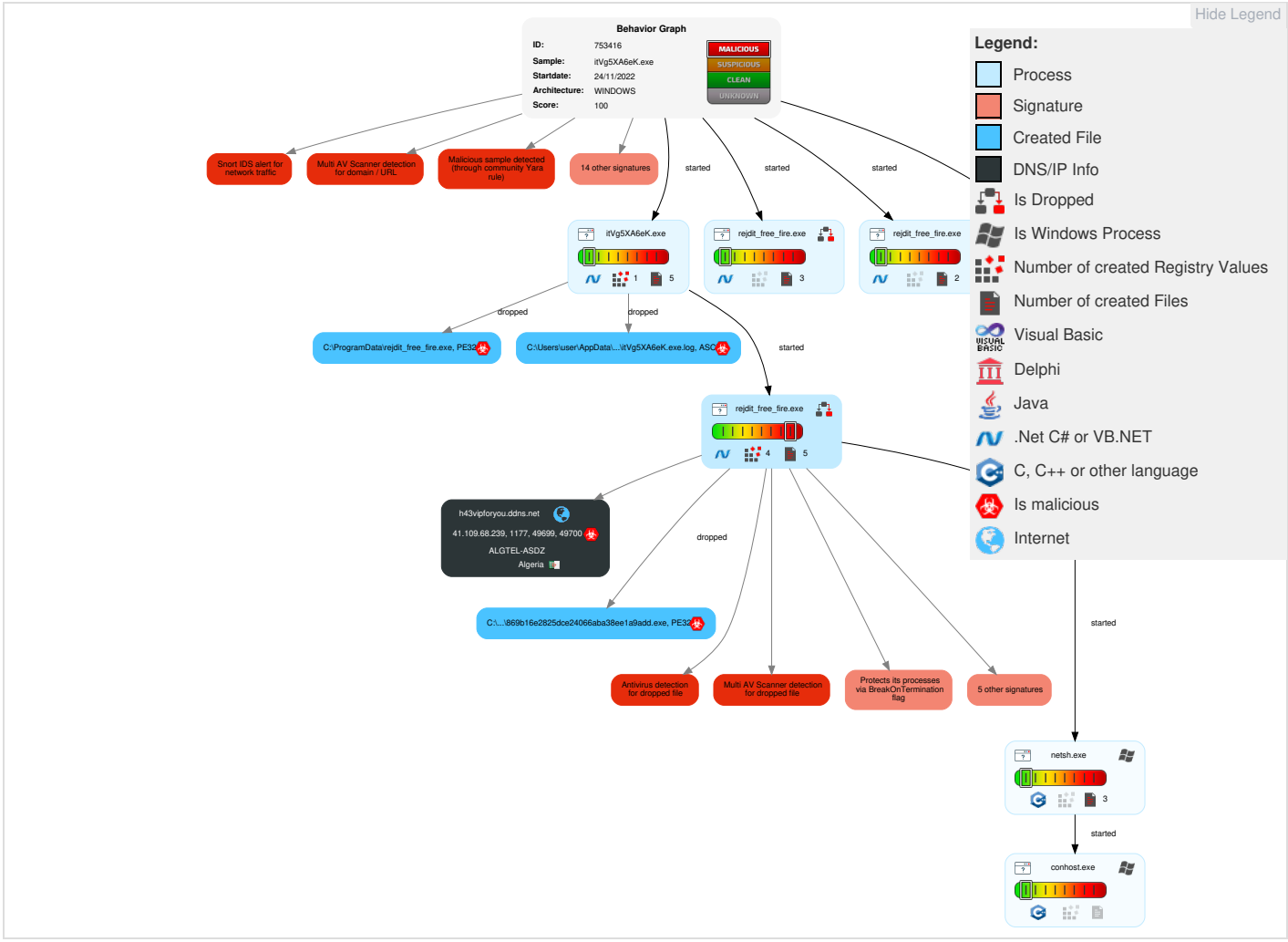
Detected njRat

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	Remote Service Effects	Impact
Valid Accounts	1 Native API	2 2 1 Registry Run Keys / Startup Folder	1 2 Process Injection	1 Masquerading	1 1 Input Capture	1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	2 2 1 Registry Run Keys / Startup Folder	2 1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

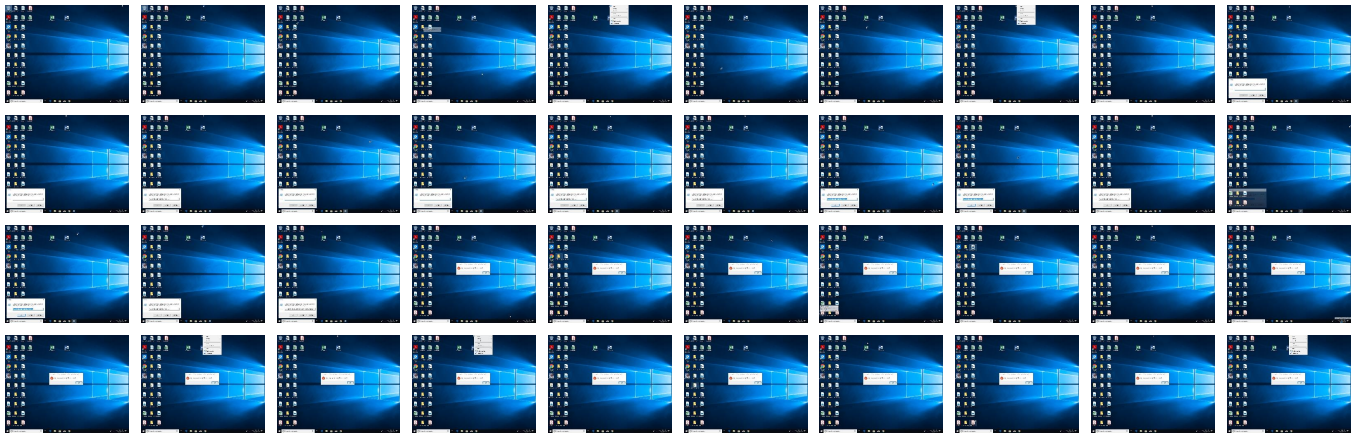
Behavior Graph



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
itVg5XA6eK.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
itVg5XA6eK.exe	76%	Virustotal		Browse
itVg5XA6eK.exe	100%	Avira	TR/Dropper.Gen7	
itVg5XA6eK.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	100%	Avira	TR/Dropper.Gen7	
C:\ProgramData\rejdit_free_fire.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	100%	Joe Sandbox ML		
C:\ProgramData\rejdit_free_fire.exe	100%	Joe Sandbox ML		
C:\ProgramData\rejdit_free_fire.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\ProgramData\rejdit_free_fire.exe	76%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	76%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.itVg5XA6eK.exe.440000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
h43vipforyou.ddns.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
h43vipforyou.ddns.net	100%	Avira URL Cloud	malware	
h43vipforyou.ddns.net	10%	Virustotal		Browse

Domains and IPs

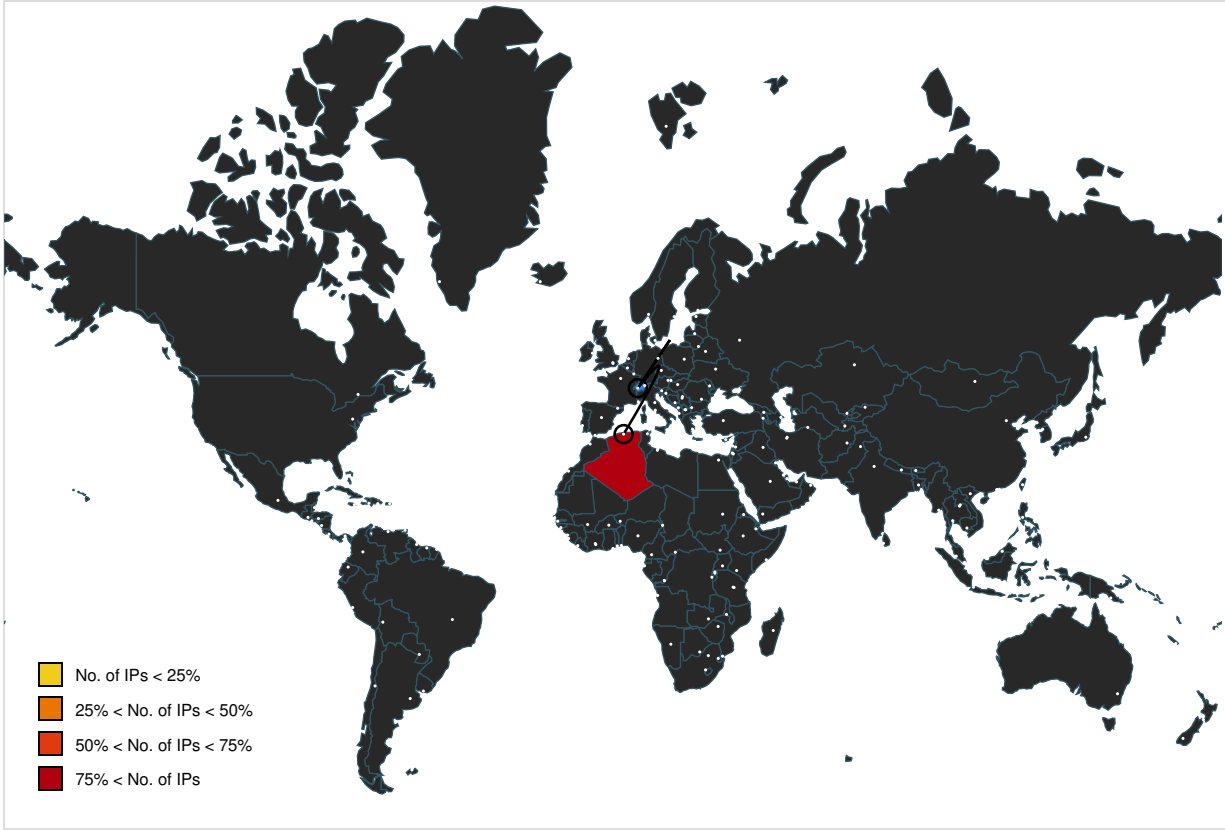
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
h43vipforyou.ddns.net	41.109.68.239	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
h43vipforyou.ddns.net	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.109.68.239	h43vipforyou.ddns.net	Algeria		36947	ALGTEL-ASDZ	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753416
Start date and time:	2022-11-24 19:41:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	itVg5XA6eK.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@9/5@4/1
EGA Information:	• Successful, ratio: 60%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 93.184.221.240
- Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Execution Graph export aborted for target rejdit_free_fire.exe, PID 1280 because it is empty
- Execution Graph export aborted for target rejdit_free_fire.exe, PID 644 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:42:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 869b16e2825dce24066aba38ee1a9add "C:\ProgramData\rejdit_free_fire.exe" ..
19:42:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 869b16e2825dce24066aba38ee1a9add "C:\ProgramData\rejdit_free_fire.exe" ..
19:42:37	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 869b16e2825dce24066aba38ee1a9add "C:\ProgramData\rejdit_free_fire.exe" ..
19:42:45	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\rejdit_free_fire.exe

Process:	C:\Users\user\Desktop\itVg5XA6eK.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	232960
Entropy (8bit):	6.66426413554523

Encrypted:	false
SSDEEP:	3072:HSuZ00DVrF1rVcCPP+Tl6Ws5cUYTMExjHSTdMTfNlx35eRPG+79IwGrpc:J/2TAcZyOjNlri7Ww
MD5:	8533EF6F79E259E9E5FE7C28F1FCD372
SHA1:	48C1F9B2A798A374B6E8C2E5FB655C19E5FA2ED3
SHA-256:	BBC8CABC1BA4F81D1EE316D3869ED8E61C91840CB533ABEE708A3099AB196470
SHA-512:	533FACB9E64028915336F7A7035E726409279309B05D2CF1E6DEF878513A85F49A9119F09E53BCC8371FF5BC8F91474B67934773E3C6A7AD12C3778FFA3F2697
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\ProgramData\rejdit_free_fire.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\ProgramData\rejdit_free_fire.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\ProgramData\rejdit_free_fire.exe, Author: Brian Wallace @botnet_hunter • Rule: Windows_Trojan_Njrat_30f3c220, Description: unknown, Source: C:\ProgramData\rejdit_free_fire.exe, Author: unknown • Rule: Njrat, Description: detect njRAT in memory, Source: C:\ProgramData\rejdit_free_fire.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100% • Antivirus: Virustotal, Detection: 76%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R[vc.....V...6.....t... .....@.. ....@.....\t..O.....d2..... ....H.....text....T... ...V..... ..`.rsrc...d2.....4...X.....@..@.rel oc.....@..B.....t.....H.....,K..0)...../.....0.....r...p.....r...p.....r...p.....rG..p.....rg..p.....r...p.....r...p.....r...p.....r...p(.... .....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....rQ..p.....*...0..;.....~....o....o....rS..p~....(....o.....o.....%(.....(.....*.....,,..... .0..D.....~....o....o....rS..p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\itVg5XA6eK.exe.log

Process:	C:\Users\user\Desktop\itVg5XA6eK.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:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5I 3
Malicious:	**true**
Reputation:	high, 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.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rejdit_free_fire.exe.log

Process:	C:\ProgramData\rejdit_free_fire.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:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5I 3
Malicious:	false
Reputation:	high, 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.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe

Process:	C:\ProgramData\rejdit_free_fire.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	232960
Entropy (8bit):	6.66426413554523
Encrypted:	false
SSDEEP:	3072:HSuZ00DVrF1rVcCPP+Tl6Ws5cUYTMExjHSTdMTfNlx35eRPG+79IwGrpc:J/2TAcZyOjNlri7Ww
MD5:	8533EF6F79E259E9E5FE7C28F1FCD372
SHA1:	48C1F9B2A798A374B6E8C2E5FB655C19E5FA2ED3
SHA-256:	BBC8CABC1BA4F81D1EE316D3869ED8E61C91840CB533ABEE708A3099AB196470
SHA-512:	533FACB9E64028915336F7A7035E726409279309B05D2CF1E6DEF878513A85F49A9119F09E53BCC8371FF5BC8F91474B67934773E3C6A7AD12C3778FFA3F2697
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe, Author: Brian Wallace @botnet_hunter • Rule: Windows_Trojan_Njrat_30f3c220, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe, Author: unknown • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100% • Antivirus: Virustotal, Detection: 76%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R[vc.....V...6.....t... .....@.. ....@.....\t..O.....d2..... ....H.....text....T... ...V..... ..`.rsrc...d2.....4...X.....@..@.reloc.....@..B.....t.....H.....,K..0)...../.....0.....r...p.....r...p.....r...p.....rG..p.....rg..p.....r...p.....r...p.....r...p.....r...p(.....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....rQ..p.....*...0..;.....~....o....o....rS..p~....(.....o.....o.....%(.....(.....*.....,,.....0..D.....~....o....o....rS..p~....(....o.....(....o.....

\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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.66426413554523
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	itVg5XA6eK.exe
File size:	232960
MD5:	8533ef6f79e259e9e5fe7c28f1fcd372
SHA1:	48c1f9b2a798a374b6e8c2e5fb655c19e5fa2ed3

SHA256:	bbc8cabc1ba4f81d1ee316d3869ed8e61c91840cb533abee708a3099ab196470
SHA512:	533facb9e64028915336f7a7035e726409279309b05d2cf1e6def878513a85f49a9119f09e53bcc8371ff5bc8f91474b67934773e3c6a7ad12c3778ffa3f2697
SSDEEP:	3072:HSuZ00DVrF1rVcCPP+Tl6Ws5cUYTMExjHSTdMTfNlx35eRPG+79IwGrpc:J/2TAcZyOjNlri7Ww
TLSH:	4834BF821D4689E8EC7E1934102D1C4EC271DD3B85B62DDA9FCAF464C9B31E1606EA7F
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...R[vc.................V...6.......t... ....@.. ....@................................

File Icon

	
Icon Hash:	33f995df0f063033

Static PE Info

General

Entrypoint:	0x4074ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63765B52 [Thu Nov 17 16:03:30 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x745c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x33264	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x54b4	0x5600	False	0.4898255813953488	data	5.58038459164499	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x33264	0x33400	False	0.6070121951219513	data	6.562617643019481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3c000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x80e8	0x32f80	Device independent bitmap graphic, 226 x 446 x 32, image size 201592		
RT_GROUP_ICON	0x3b068	0x14	data		
RT_MANIFEST	0x3b07c	0x1e7	XML 1.0 document, ASCII text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

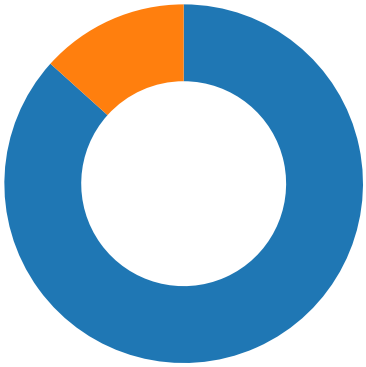
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.341.109.68.239 4969911772033132 11/24/22-19:42:23.177340	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49699	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4969911772825563 11/24/22-19:42:23.319941	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49699	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970111772825563 11/24/22-19:43:29.909277	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49701	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970011772033132 11/24/22-19:42:56.789376	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49700	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4969911772825564 11/24/22-19:42:28.743067	TCP	2825564	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)	49699	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970011772825564 11/24/22-19:43:01.745518	TCP	2825564	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)	49700	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970011772825563 11/24/22-19:42:56.884058	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49700	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970111772033132 11/24/22-19:43:29.805466	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49701	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970111772814856 11/24/22-19:43:29.909277	TCP	2814856	ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf)	49701	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970211772825563 11/24/22-19:44:02.683537	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49702	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970111772814860 11/24/22-19:43:44.045655	TCP	2814860	ETPRO TROJAN njRAT/Bladabindi CnC Callback (act)	49701	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970211772033132 11/24/22-19:44:02.583206	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49702	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4969911772814860 11/24/22-19:42:28.743067	TCP	2814860	ETPRO TROJAN njRAT/Bladabindi CnC Callback (act)	49699	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970211772814856 11/24/22-19:44:02.683537	TCP	2814856	ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf)	49702	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970011772814860 11/24/22-19:43:01.745518	TCP	2814860	ETPRO TROJAN njRAT/Bladabindi CnC Callback (act)	49700	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970111772825564 11/24/22-19:43:44.045655	TCP	2825564	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)	49701	1177	192.168.2.3	41.109.68.239
192.168.2.341.109.68.239 4970011772814856 11/24/22-19:42:56.884058	TCP	2814856	ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf)	49700	1177	192.168.2.3	41.109.68.239

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.341.109.68.239 4969911772814856 11/24/22-19:42:23.319941	TCP	2814856	ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf)	49699	1177	192.168.2.3	41.109.68.239

Network Port Distribution



Total Packets: 30

- 53 (DNS)
- 1177 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:42:22.877197981 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:22.978322029 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:22.978456974 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:23.177340031 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:23.319797993 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:23.319941044 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:23.475019932 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:28.743067026 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:29.029788017 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:53.837865114 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:53.838188887 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.635041952 CET	49699	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.703151941 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.742235899 CET	1177	49699	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:56.776344061 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:56.776509047 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.789376020 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.883812904 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:42:56.884057999 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:42:56.986124992 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:01.745517969 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:01.860215902 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:27.425684929 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:27.425894976 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:29.566560984 CET	49700	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:29.634968042 CET	1177	49700	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:29.699424028 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:29.769546032 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:29.769810915 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:29.805465937 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:29.909079075 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:29.909276962 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:30.009236097 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:35.919970989 CET	49701	1177	192.168.2.3	41.109.68.239

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:43:36.018954992 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:43:44.045655012 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:43:44.143486023 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:44:00.425215006 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:44:00.425400019 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.437489986 CET	49701	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.491133928 CET	49702	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.504364014 CET	1177	49701	41.109.68.239	192.168.2.3
Nov 24, 2022 19:44:02.563647032 CET	1177	49702	41.109.68.239	192.168.2.3
Nov 24, 2022 19:44:02.563779116 CET	49702	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.583205938 CET	49702	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.682976007 CET	1177	49702	41.109.68.239	192.168.2.3
Nov 24, 2022 19:44:02.683537006 CET	49702	1177	192.168.2.3	41.109.68.239
Nov 24, 2022 19:44:02.784684896 CET	1177	49702	41.109.68.239	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:42:22.846184969 CET	49977	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:42:22.867410898 CET	53	49977	8.8.8.8	192.168.2.3
Nov 24, 2022 19:42:56.673460960 CET	57840	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:42:56.691323042 CET	53	57840	8.8.8.8	192.168.2.3
Nov 24, 2022 19:43:29.652144909 CET	57990	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:43:29.674014091 CET	53	57990	8.8.8.8	192.168.2.3
Nov 24, 2022 19:44:02.472203970 CET	52387	53	192.168.2.3	8.8.8.8
Nov 24, 2022 19:44:02.489883900 CET	53	52387	8.8.8.8	192.168.2.3

DNS Queries

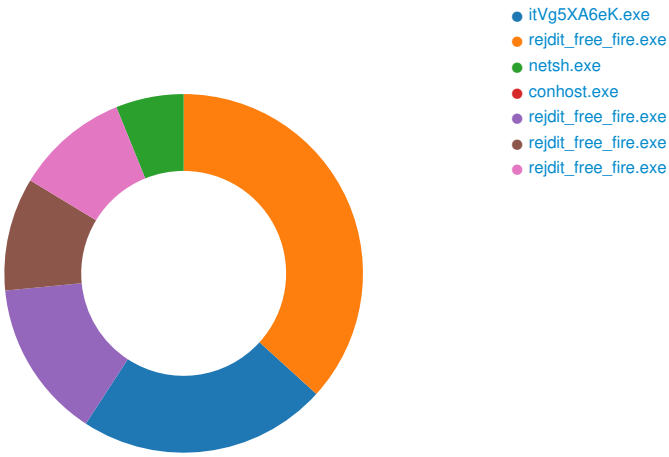
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 19:42:22.846184969 CET	192.168.2.3	8.8.8.8	0x2f59	Standard query (0)	h43vipfory ou.ddns.net	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:42:56.673460960 CET	192.168.2.3	8.8.8.8	0x243b	Standard query (0)	h43vipfory ou.ddns.net	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:43:29.652144909 CET	192.168.2.3	8.8.8.8	0xa7fd	Standard query (0)	h43vipfory ou.ddns.net	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:44:02.472203970 CET	192.168.2.3	8.8.8.8	0x8aba	Standard query (0)	h43vipfory ou.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 19:42:22.867410898 CET	8.8.8.8	192.168.2.3	0x2f59	No error (0)	h43vipfory ou.ddns.net		41.109.68.239	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:42:56.691323042 CET	8.8.8.8	192.168.2.3	0x243b	No error (0)	h43vipfory ou.ddns.net		41.109.68.239	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:43:29.674014091 CET	8.8.8.8	192.168.2.3	0xa7fd	No error (0)	h43vipfory ou.ddns.net		41.109.68.239	A (IP address)	IN (0x0001)	false
Nov 24, 2022 19:44:02.489883900 CET	8.8.8.8	192.168.2.3	0x8aba	No error (0)	h43vipfory ou.ddns.net		41.109.68.239	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: itVg5XA6eK.exe PID: **6104**, Parent PID: **3452**

General

Target ID:	0
Start time:	19:41:59
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\itVg5XA6eK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\itVg5XA6eK.exe
Imagebase:	0x440000
File size:	232960 bytes
MD5 hash:	8533EF6F79E259E9E5FE7C28F1FCD372
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Windows_Trojan_Njrat_30f3c220, Description: unknown, Source: 00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.255333528.0000000003AB4000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000000.239853870.0000000000442000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000000.239853870.0000000000442000.00000002.00000001.01000000.00000003.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Windows_Trojan_Njrat_30f3c220, Description: unknown, Source: 00000000.00000000.239853870.0000000000442000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000000.239853870.0000000000442000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\ProgramData\rejdit_free_fire.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	D4AA07	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\itVg5XA6eK.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	729A34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\rejdit_free_fire.exe	0	232960	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 52 5b 76 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 56 00 00 00 36 03 00 00 00 00 00 fd 74 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELR[vcV6t @ @	success or wait	1	D4AC8F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\itVg5XA6eK.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72C8A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
C:\Users\user\Desktop\itVg5XA6eK.exe	unknown	232960	success or wait	1	D4AC8F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	D4A4FA	RegSetValueExW

Analysis Process: rejdit_free_fire.exe PID: **1852**, Parent PID: **6104**

General

Target ID:	1
Start time:	19:42:06
Start date:	24/11/2022
Path:	C:\ProgramData\rejdit_free_fire.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\rejdit_free_fire.exe"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	8533EF6F79E259E9E5FE7C28F1FCD372
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000001.00000002.507753585.0000000002965000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\ProgramData\rejdit_free_fire.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\ProgramData\rejdit_free_fire.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\ProgramData\rejdit_free_fire.exe, Author: Brian Wallace @botnet_hunter • Rule: Windows_Trojan_Njrat_30f3c220, Description: unknown, Source: C:\ProgramData\rejdit_free_fire.exe, Author: unknown • Rule: Njrat, Description: detect njRAT in memory, Source: C:\ProgramData\rejdit_free_fire.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, ReversingLabs • Detection: 76%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71F793EB	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\869b16e2825dce24066aba38ee1a9add.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 52 5b 76 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 56 00 00 00 36 03 00 00 00 00 00 fd 74 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELR[vcV6t @ @	success or wait	2	71F793EB	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	A80BE3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	A80BE3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\869b16e2825dce24066aba38ee1a9add	success or wait	1	A82C1F	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Environment	SEE_MASK_NOZONECHECKS	unicode	1	success or wait	1	71FBC863	unknown
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	869b16e2825dce24066aba38ee1a9add	unicode	"C:\ProgramData\rejdit_free_fire.exe" ..	success or wait	1	71FBC863	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	869b16e2825dce24066aba38ee1a9add	unicode	"C:\ProgramData\rejdit_free_fire.exe" ..	success or wait	1	71FBC863	unknown
HKEY_CURRENT_USER\Software\869b16e2825dce24066aba38ee1a9add	[kl]	unicode		success or wait	1	71FBC863	unknown

Analysis Process: netsh.exe PID: **2436**, Parent PID: **1852**

General

Target ID:	2
Start time:	19:42:14
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram "C:\ProgramData\rejdit_free_fire.exe" "rejdit_free_fire.exe" ENABLE
Imagebase:	0x10f0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	306	306	4f 6b 2e 0d 0a 0d 0a	Ok.	success or wait	1	10F7B1B	WriteFile
\Device\ConDrv	311	5	0d 0a		success or wait	1	10F7B1B	WriteFile
\Device\ConDrv	313	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	10F7B1B	WriteFile

Analysis Process: conhost.exe PID: **732**, Parent PID: **2436**

General

Target ID:	3
Start time:	19:42:15
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: rejdit_free_fire.exe PID: **644**, Parent PID: **3452**

General

Target ID:	13
Start time:	19:42:29
Start date:	24/11/2022
Path:	C:\ProgramData\rejdit_free_fire.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\rejdit_free_fire.exe" ..
Imagebase:	0x670000
File size:	232960 bytes
MD5 hash:	8533EF6F79E259E9E5FE7C28F1FCD372
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rejdit_free_fire.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	729A34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\rejdit_free_fire.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72C8A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile

Analysis Process: rejdit_free_fire.exe PID: **1280**, Parent PID: **3452**

General

Target ID:	14
Start time:	19:42:37
Start date:	24/11/2022
Path:	C:\ProgramData\rejdit_free_fire.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\rejdit_free_fire.exe" ..
Imagebase:	0x980000
File size:	232960 bytes
MD5 hash:	8533EF6F79E259E9E5FE7C28F1FCD372
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile

Analysis Process: rejdit_free_fire.exe PID: **1112**, Parent PID: **3452**

General

Target ID:	15
Start time:	19:42:45
Start date:	24/11/2022
Path:	C:\ProgramData\rejdit_free_fire.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\rejdit_free_fire.exe" ..
Imagebase:	0xd70000
File size:	232960 bytes

MD5 hash:	8533EF6F79E259E9E5FE7C28F1FCD372
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	729B60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile

Disassembly

No disassembly