ID: 736964
Sample Name: U8RYIwIvfK.exe
Cookbook: default.jbs
Time: 12:38:55
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

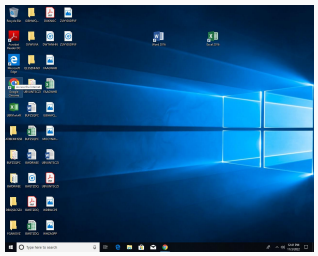
Windows Analysis Report

U8RYIwIvfK.exe

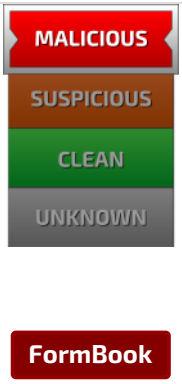
Overview

General Information

Sample Name:	U8RYIwIvfK.exe
Analysis ID:	736964
MD5:	6f53598b9c19b3..
SHA1:	4bd8e67e468adf..
SHA256:	6d3397c687aea5..
Tags:	exe Formbook
Infos:	



Detection



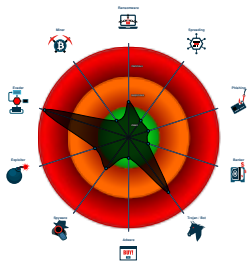
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- .NET source code references suspic…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- U8RYIwIvfK.exe (PID: 5840 cmdline: C:\Users\user\Desktop\U8RYIwIvfK.exe MD5: 6F53598B9C19B30A0CF3FF0432301708)
  - aspnet_compiler.exe (PID: 5140 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
  - aspnet_compiler.exe (PID: 6124 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
  - aspnet_compiler.exe (PID: 6120 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 5916 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 4120 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ept-egy.com/zx85/"
  ],
  "decoy": [
    "myclassly.com",
    "rilcon.xyz",
    "miracleun.shop",
    "gadgetward-usa.com",
    "farmaacademy.com",
    "dreamsolutions.group",
    "fffood.online",
    "ziggnl.site",
    "cherpol.com",
    "imprescriptible-tienoscope.biz",
    "yztc.fun",
    "chicagonftweek.com",
    "zz0659.com",
    "hznaixi.com",
    "027-seo.net",
    "korlekded.com",
    "gelatoitaly.com",
    "finlitguru.com",
    "gupingapp.com",
    "manmakecoffee.com",
    "yuanwei.lol",
    "cargovoyager.com",
    "getjobzz.com",
    "dagatructiephd.com",
    "mynab.mobi",
    "masteralbert.com",
    "rtugwmt0cs.vip",
    "uscanvas.net",
    "nocrytech.com",
    "canadaroi.com",
    "archivegamer.com",
    "crossinspectionservices.com",
    "dxxws.com",
    "rufflyfedogtraining.com",
    "prgrn.dev",
    "bwdcourses.com",
    "criptomexico.com",
    "elisabethingram.online",
    "drationa.shop",
    "pulsarthermalscope.shop",
    "grcpp8vyuk.vip",
    "sh-whyyl.com",
    "in-cdn.xyz",
    "aquatabdouro.online",
    "handsomeshooterjewelry.com",
    "erug.store",
    "trueimpact.studio",
    "taskalso.com",
    "dzslqdz.xyz",
    "barbushing.com",
    "freightxpert.com",
    "777703.xyz",
    "bradysproducts.com",
    "teensforcp.site",
    "gpssystemecuador.com",
    "luxslides.com",
    "sony8ktv.monster",
    "baxiservisim.xyz",
    "lojascacau.com",
    "sfanci.com",
    "magdrade.com",
    "jobreadyfresher.com",
    "dori-maniacs.com",
    "mercydm.mobi"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bbb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x99bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x958a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17839:$sqlite3step: 68 34 1C 7B E1 • 0x1794c:$sqlite3step: 68 34 1C 7B E1 • 0x17868:$sqlite3text: 68 38 2A 90 C5 • 0x1798d:$sqlite3text: 68 38 2A 90 C5 • 0x1787b:$sqlite3blob: 68 53 D8 7F 8C • 0x179a3:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.518748658.0000000000120000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.aspnet_compiler.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bbf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14aa7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.0.aspnet_compiler.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.aspnet_compiler.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Windows executable base64 encoded - Source IP: 50.115.174.192 - Destination IP: 192.168.2.6

Timestamp:	50.115.174.192192.168.2.6443497042018856 11/03/22-12:39:59.450093
SID:	2018856
Source Port:	443
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a .tk domain - Likely Hostile - Source IP: 192.168.2.6 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.68.8.8.859575532012811 11/03/22-12:39:56.025984
SID:	2012811
Source Port:	59575
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

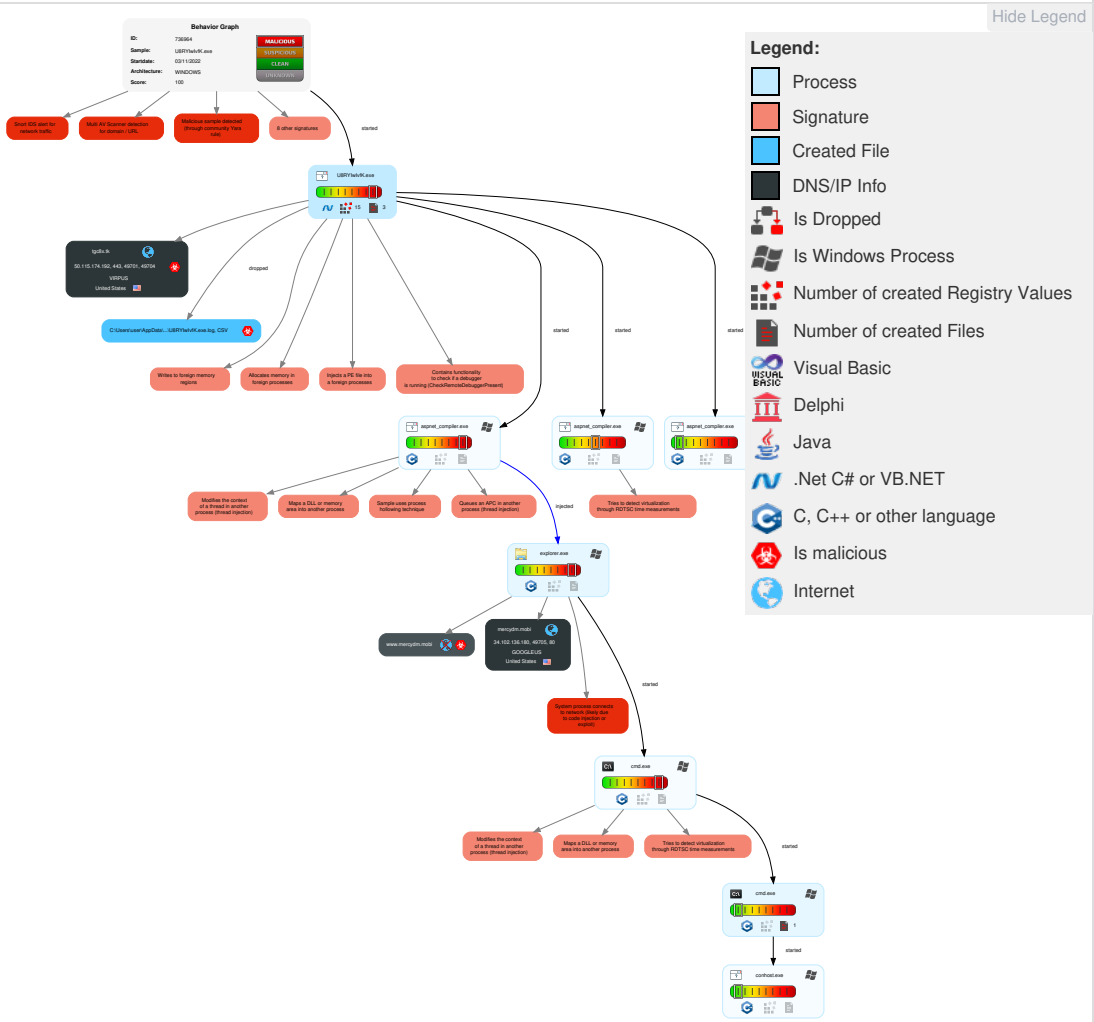
Yara detected FormBook

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
1 Valid Accounts	1 Native API	1 Valid Accounts	1 Valid Accounts	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Masquerading	LSASS Memory	2 4 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	8 1 2 Process Injection	1 Valid Accounts	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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 Access Token Manipulation	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Disable or Modify Tools	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	3 1 Virtualization/Sandbox Evasion	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	8 1 2 Process Injection	DCSync	1 2 5 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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Deobfuscate/Decode Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 Obfuscated Files or Information	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 1 Software Packing	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

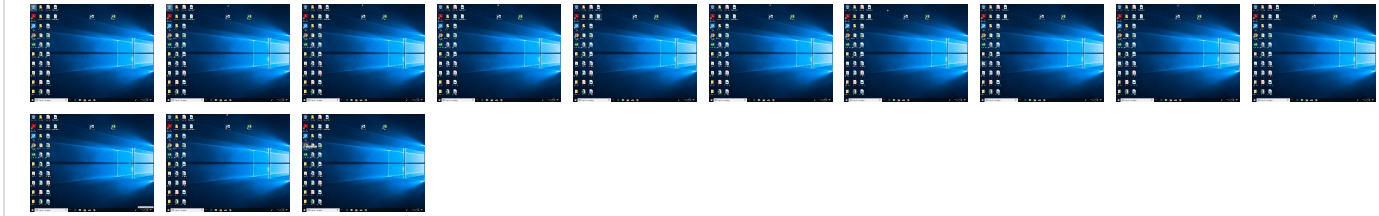
Behavior Graph



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
U8RYIwIvfK.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
U8RYIwIvfK.exe	38%	Virustotal		Browse
U8RYIwIvfK.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
tgc8x.tk	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://tgc8x.tk/tt/ptrr.txt	3%	Virustotal		Browse
http://https://tgc8x.tk	7%	Virustotal		Browse
http://www.mercydm.mobi/zx85/?Sl=JSAN+BGUWbFlio0Y6cR2moHwDIFZVOq3R3uV7C0AfntmXLYJvKIE34aC+rLPWCkZ7Yk0ST8b/A==&7ntH=U0D8yn_PIXqTt	0%	Avira URL Cloud	safe	
http://https://tgc8x.tk	0%	Avira URL Cloud	safe	
www.ept-egy.com/zx85/	0%	Virustotal		Browse
www.ept-egy.com/zx85/	0%	Avira URL Cloud	safe	
http://tgc8x.tk	0%	Avira URL Cloud	safe	
http://https://tgc8x.tk/tt/ptrr.txt	100%	Avira URL Cloud	phishing	
http://https://tgc8x.tkD8	0%	Avira URL Cloud	safe	
http://https://tgc8x.tk4	0%	Avira URL Cloud	safe	
http://https://tgc8x.tk/tt/BLACKDEV.txt	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tgc8x.tk	50.115.174.192	true	true	• 6%, Virustotal, Browse	unknown
mercydm.mobi	34.102.136.180	true	false		unknown
www.mercydm.mobi	unknown	unknown	true		unknown

Contacted URLs

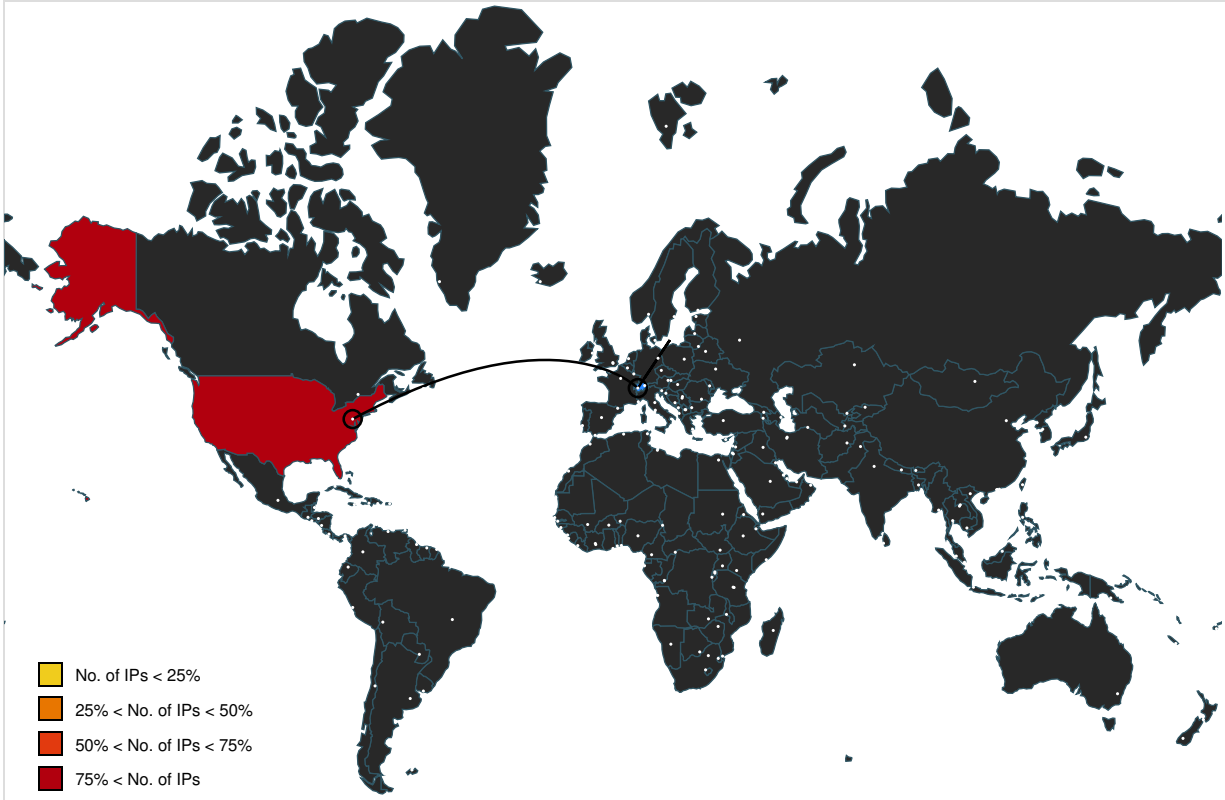
Name	Malicious	Antivirus Detection	Reputation
http://https://tgc8x.tk/tt/BLACKDEV.txt	true	• Avira URL Cloud: phishing	unknown
http://https://tgc8x.tk/tt/ptrr.txt	true	• 3%, Virustotal, Browse • Avira URL Cloud: phishing	unknown
www.ept-egy.com/zx85/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low
http://www.mercydm.mobi/zx85/?Sl=JSAN+BGUWbFlio0Y6cR2moHwDIFZVOq3R3uV7C0AfntmXLYJvKIE34aC+rLPWCkZ7Yk0ST8b/A==&7ntH=U0D8yn_PIXqTt	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.29568684 3.0000000008442000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.352239311.0000000008442000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.315487552.000000 0000AC8000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0000.270907548.0000000000AC8000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.341973422.0000000000AC80 00.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://tgc8x.tk	U8RYIwIvfK.exe, 00000000.00000002.267402 025.0000000002661000.00000004.00000800.0 0020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tgc8x.tk4	U8RYIwIvfK.exe, 00000000.00000002.267402025.0000000002661000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	U8RYIwIvfK.exe, 00000000.00000002.267402025.0000000002661000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tgc8x.tk	U8RYIwIvfK.exe, 00000000.00000002.267602853.0000000002677000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://tgc8x.tkD8	U8RYIwIvfK.exe, 00000000.00000002.268543578.0000000002755000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.115.174.192	tgc8x.tk	United States		32875	VIRPUS	true
34.102.136.180	mercydm.mobi	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736964
Start date and time:	2022-11-03 12:38:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	U8RYIwIvfK.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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/1@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.4% (good quality ratio 54.2%) • Quality average: 70.2% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 99% • 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
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:40:00	API Interceptor	1x Sleep call for process: U8RYIwIvfK.exe modified

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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\U8RYIwIvfK.exe.log

Process:	C:\Users\user\Desktop\U8RYIwIvfK.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.8598559767101115
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	U8RYIwIvfK.exe
File size:	74240
MD5:	6f53598b9c19b30a0cf3ff0432301708
SHA1:	4bd8e67e468adfbfddd9e5a1e47fdf318bf9a31b
SHA256:	6d3397c687aea5017b90a5e96adc6fbfb0429d56a8b2ead1f1d4273994952379
SHA512:	e655648f950b90261fd2b54be1ebfee9780ff466351d1cc4b1a675c41329fc5eae62f20ccb9423d3ee4e3457c7a8ed63b14bc2e30f205a4512122301ce2d1541
SSDEEP:	1536:7BKK5PX8Q01Hb20oJ0fekpamVGfhCW7j:lKSx0177ouekpamVGfhCW7j
TLSH:	E573EC8D766071DFC85BC872CEA82C68EA64747B531BD203A45326AD9E0D99BCF150F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....;cc.....0.....%... ...@....@.. .....w%...`.....

File Icon

Icon Hash:	30f0c4ccccc6b010

Static PE Info

General

Entrypoint:	0x4125ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63633BBE [Thu Nov 3 03:55:42 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x125a0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1746	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x12558	0x1c	.text
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	0x105f4	0x10600	False	0.4767861402671756	data	5.884370189804151	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1746	0x1800	False	0.2711588541666667	data	4.422035362903512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x16000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14164	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_GROUP_ICON	0x1520c	0x14	data		
RT_VERSION	0x15220	0x33c	data		
RT_MANIFEST	0x1555c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

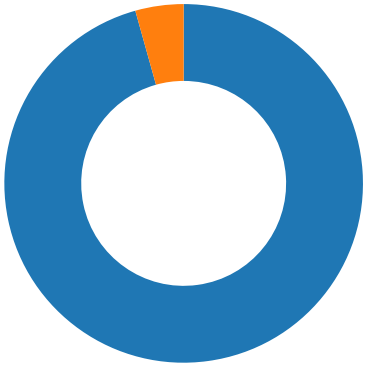
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
50.115.174.192192.168.2.6443497042018856 11/03/22-12:39:59.450093	TCP	2018856	ET TROJAN Windows executable base64 encoded	443	49704	50.115.174.192	192.168.2.6
192.168.2.68.8.8.8595755 32012811 11/03/22-12:39:56.025984	UDP	2012811	ET DNS Query to a .tk domain - Likely Hostile	59575	53	192.168.2.6	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:39:56.396153927 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:56.396225929 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:56.396327019 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:56.450129986 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:56.450177908 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:56.835751057 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:56.835985899 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:56.848099947 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:56.848124027 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:56.848771095 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:56.919364929 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.640667915 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.640702009 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.819936037 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.819999933 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.820017099 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.820031881 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.820125103 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.820158958 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.872545004 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.997368097 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997410059 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997458935 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997530937 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.997567892 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997567892 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.997586012 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997622967 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997632027 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.997632980 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:57.997662067 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:57.997689962 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.175142050 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175272942 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175385952 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175427914 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175431013 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.175487995 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.175502062 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175551891 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175565958 CET	49701	443	192.168.2.6	50.115.174.192

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:39:58.175580025 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175621033 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.175745010 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.175857067 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.353627920 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.353775024 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.353818893 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.353848934 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.353869915 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.353893995 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.354007959 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.354073048 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.354207039 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.354294062 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.354432106 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.354499102 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.354631901 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.354705095 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533330917 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533480883 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533509970 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533618927 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533631086 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533655882 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533679962 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533711910 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533741951 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533799887 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533857107 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.533926964 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.533982992 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.534043074 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.534089088 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.534158945 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.534224987 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.534296036 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.534343958 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.534409046 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.534466028 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.534524918 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.712263107 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.712383032 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.712660074 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.712667942 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.712697983 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.712798119 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.712939024 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713038921 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.713177919 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713260889 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.713460922 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713546991 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.713736057 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713886976 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713890076 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.713900089 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.713972092 CET	49701	443	192.168.2.6	50.115.174.192
Nov 3, 2022 12:39:58.713978052 CET	443	49701	50.115.174.192	192.168.2.6
Nov 3, 2022 12:39:58.714051962 CET	49701	443	192.168.2.6	50.115.174.192

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:39:56.025984049 CET	59575	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:39:56.357557058 CET	53	59575	8.8.8.8	192.168.2.6
Nov 3, 2022 12:41:36.152439117 CET	58595	53	192.168.2.6	8.8.8.8
Nov 3, 2022 12:41:36.184751987 CET	53	58595	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:39:56.025984049 CET	192.168.2.6	8.8.8.8	0x1cce	Standard query (0)	tgc8x.tk	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:41:36.152439117 CET	192.168.2.6	8.8.8.8	0x7240	Standard query (0)	www.mercydm.mobi	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 3, 2022 12:39:56.357557058 CET	8.8.8.8	192.168.2.6	0x1cce	No error (0)	tgc8x.tk		50.115.174.192	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:41:36.184751987 CET	8.8.8.8	192.168.2.6	0x7240	No error (0)	www.mercydm.mobi	mercydm.mobi		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:41:36.184751987 CET	8.8.8.8	192.168.2.6	0x7240	No error (0)	mercydm.mobi		34.102.136.180	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- tgc8x.tk
- www.mercydm.mobi

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

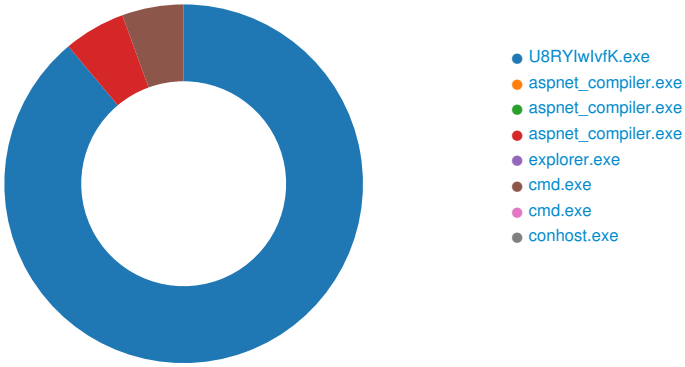
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE9
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE9
GetMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE9
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE9

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: U8RYIwIvfK.exe PID: **5840**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:39:53
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\U8RYIwIvfK.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\U8RYIwIvfK.exe
Imagebase:	0x240000
File size:	74240 bytes
MD5 hash:	6F53598B9C19B30A0CF3FF0432301708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.268793282.0000000003668000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.268793282.0000000003668000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.268793282.0000000003668000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.268793282.0000000003668000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: aspnet_compiler.exe PID: **5140**, Parent PID: **5840**

General

Target ID:	1

Start time:	12:39:59
Start date:	03/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x120000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: **6124**, Parent PID: **5840**

General

Target ID:	2
Start time:	12:39:59
Start date:	03/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x3c0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: **6120**, Parent PID: **5840**

General

Target ID:	3
Start time:	12:39:59
Start date:	03/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x6a0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.265897540.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **6120**

General

Target ID:	4
Start time:	12:40:02
Start date:	03/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.333824119.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.333824119.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.333824119.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.333824119.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.354984308.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.354984308.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.354984308.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.354984308.000000000E1A1000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5916**, Parent PID: **3452**

General

Target ID:	14
Start time:	12:40:44
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.518748658.0000000000120000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.518748658.0000000000120000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.518748658.0000000000120000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.518748658.0000000000120000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.521754636.0000000002AE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.521754636.0000000002AE0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.521754636.0000000002AE0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.521754636.0000000002AE0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.520146703.00000000023A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000002.520146703.00000000023A0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.520146703.00000000023A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.520146703.00000000023A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	13A447	NtReadFile

Analysis Process: cmd.exe PID: **4120**, Parent PID: **5916**

General

Target ID:	15
Start time:	12:40:49
Start date:	03/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5256**, Parent PID: **4120**

General

Target ID:	16
Start time:	12:40:49
Start date:	03/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly