ID: 620775
Sample Name: Ay9xkK3NYN
Cookbook: default.jbs
Time: 08:10:33
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Ay9xkK3NYN 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Temp\ptcgl43g463vgbr58 12
C:\Users\user\AppData\Local\Temp\rysgtozci.exe 13
C:\Users\user\AppData\Local\Temp\wduqqtzg 13
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Rich Headers 15
Data Directories 15
Sections 16
Resources 16
Imports 16
Possible Origin 16
Network Behavior 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
Code Manipulations 17
User Modules 17
Hook Summary 17
Processes 17

Statistics 17
Behavior 17
System Behavior 18
Analysis Process: Ay9xkK3NYN.exePID: 6376, Parent PID: 5168 18
General 18
File Activities 18
Analysis Process: rysgtozci.exePID: 6412, Parent PID: 6376 18
General 18
File Activities 18
File Read 18
Analysis Process: rysgtozci.exePID: 6440, Parent PID: 6412 18
General 18
File Activities 19
File Read 19
Analysis Process: explorer.exePID: 684, Parent PID: 6440 19
General 19
File Activities 20
Analysis Process: systray.exePID: 3060, Parent PID: 684 20
General 20
File Activities 20
File Read 20
Analysis Process: cmd.exePID: 3348, Parent PID: 3060 20
General 20
File Activities 21
Analysis Process: conhost.exePID: 6652, Parent PID: 3348 21
General 21
Disassembly 21

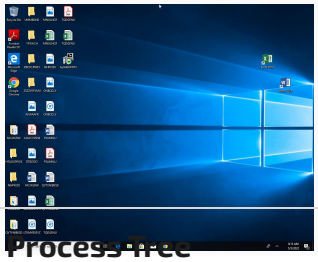
Windows Analysis Report

Ay9xkK3NYN

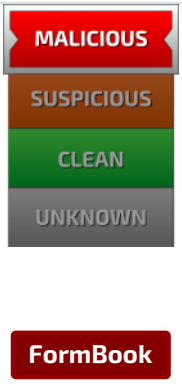
Overview

General Information

Sample Name:	Ay9xkK3NYN (renamed file extension from none to exe)
Analysis ID:	620775
MD5:	5fc986129c3d83…
SHA1:	2ace6bc0488df9…
SHA256:	d02d076842cc94…
Tags:	32 exe Formbook trojan
Infos:	



Detection



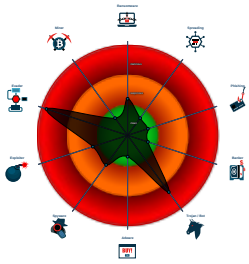
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Tries to detect virtualization through…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- Ay9xkK3NYN.exe (PID: 6376 cmdline: "C:\Users\user\Desktop\Ay9xkK3NYN.exe" MD5: 5FC986129C3D833B1C7E5BA6FF3678BC)
  - rysgtozci.exe (PID: 6412 cmdline: C:\Users\user\AppData\Local\Temp\rysgtozci.exe C:\Users\user\AppData\Local\Temp\wduqqtzg MD5: 96B3C3B0F05B4CEDF349797D7CB05627)
    - rysgtozci.exe (PID: 6440 cmdline: C:\Users\user\AppData\Local\Temp\rysgtozci.exe C:\Users\user\AppData\Local\Temp\wduqqtzg MD5: 96B3C3B0F05B4CEDF349797D7CB05627)
      - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - systray.exe (PID: 3060 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
          - cmd.exe (PID: 3348 cmdline: /c del "C:\Users\user\AppData\Local\Temp\rysgtozci.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.shishlomarket24.biz/fw02/"
  ],
  "decoy": [
    "payer-breakers.com",
    "thesiscoper.com",
    "rental-villa.com",
    "scovikinnovations.com",
    "hydh33.com",
    "allmyshit.rest",
    "lovejaclyn.com",
    "vanessaruizwriting.com",
    "dufonddelaclasse.com",
    "kiddee168.com",
    "monumentalmarketsllc.com",
    "musclegainfatloss.com",
    "avida.info",
    "cosmo-wellness.net",
    "dandelionfusedigital.com",
    "oversizeloadbanners.com",
    "konstelle.store",
    "sdjnsbd.com",
    "czoqg.xyz",
    "5p6xljjse1lq.xyz",
    "10936.loan",
    "primeiropasso.website",
    "salarydetector.net",
    "the6figureshow.com",
    "ritzluxurytransportation.com",
    "5145.design",
    "web3ido.xyz",
    "starweaverdesigns.com",
    "cbdtz.com",
    "sunwall.xyz",
    "ornitv.com",
    "curateddesignsconsulting.com",
    "businesshairways.biz",
    "willacloud.com",
    "accusecures.com",
    "hl243.com",
    "coffellc.icu",
    "eddrugs2018.com",
    "lidakang.xyz",
    "salesstorecolombia.com",
    "ilina.xyz",
    "partieslikethese.com",
    "peymantasnimi.com",
    "datthocu.xyz",
    "cybertechsolutions.xyz",
    "findy.guru",
    "trybes.space",
    "arulinks.com",
    "yuriookinoart.com",
    "largestjerseysstore.com",
    "fortitude-tech.com",
    "ywfjp.com",
    "b1v097f2avze.xyz",
    "abdullahnazhim.com",
    "zhaoav111.info",
    "cegrowing.com",
    "llaveselmuerto.com",
    "7477e.xyz",
    "chabusinessloans.com",
    "ht-brain.com",
    "app-compound.finance",
    "0085208.com",
    "wewinaccidents.com",
    "ztzfirst.xyz"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.696256426.00000000048E0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.696256426.00000000048E0000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.rysgtozci.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.rysgtozci.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.rysgtozci.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
2.2.rysgtozci.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.rysgtozci.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

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

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

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

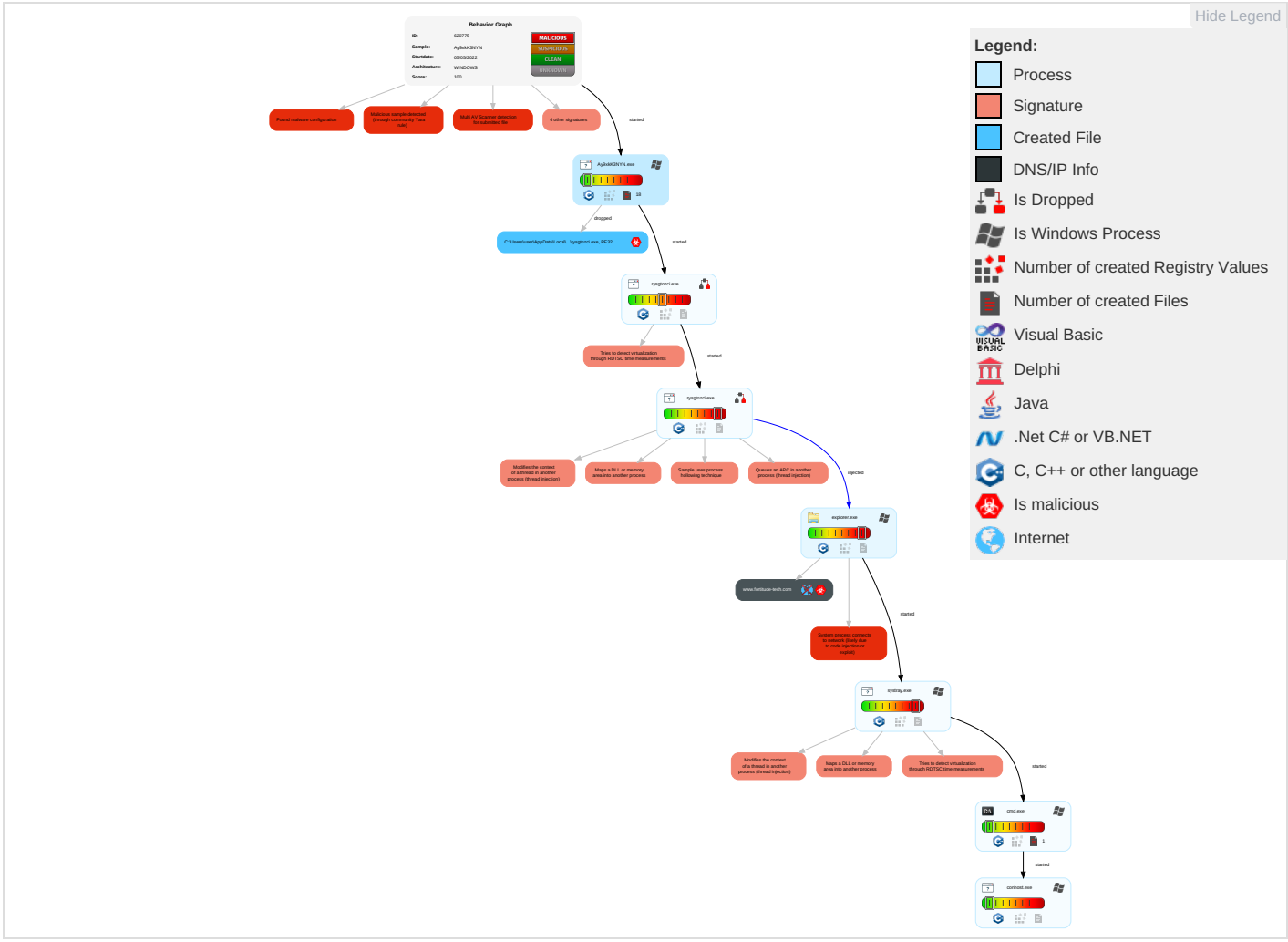
Remote Access Functionality

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
Valid Accounts	1 Shared Modules	Path Interception	1 Access Token Manipulation	1 Rootkit	1 Credential API Hooking	1 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	5 1 2 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 1 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)	5 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory 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 Obfuscated Files or Information	Cached Domain Credentials	1 3 System Information 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	1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

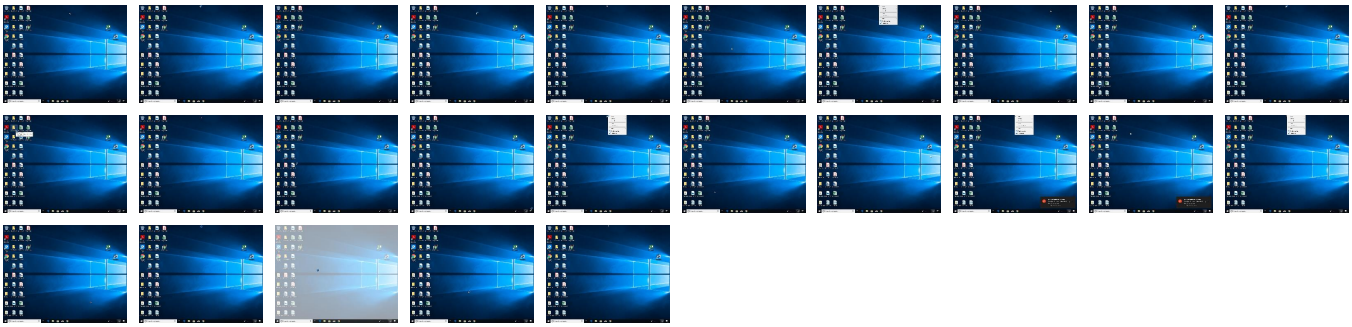
Behavior Graph



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
Ay9xkK3NYN.exe	37%	Virustotal		Browse
Ay9xkK3NYN.exe	43%	ReversingLabs	Win32.Trojan.LokiBot	
Ay9xkK3NYN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.rysgtozci.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.rysgtozci.exe.600000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.rysgtozci.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.rysgtozci.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.rysgtozci.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.shishlomarket24.biz/fw02/	0%	Virustotal		Browse
www.shishlomarket24.biz/fw02/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.fortitude-tech.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.shishlomarket24.biz/fw02/	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	Ay9xkK3NYN.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620775
Start date and time: 05/05/202208:10:33	2022-05-05 08:10:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ay9xkK3NYN (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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@9/3@1/0

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 61.7% (good quality ratio 56.7%) • Quality average: 74% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.54.89.106, 52.152.110.14, 40.125.122.176, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

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\Temp\ptcgl43g463vgbr58

Process:	C:\Users\user\Desktop\Ay9xkK3NYN.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.991393966173862**
Encrypted:	**true**

SSDEEP:	3072:4j17qN4Bvdkw8J7ApvkCao2zXSlae7jCc6g31Wy4iUCxNENtYVnqGPonTfLwJ8:4jNTvNuApvbaoiSl57jh6g31Y3raVnq1
MD5:	B5B1C1F4818202956B29108FB25DEC20
SHA1:	7E74A79237D3090B0DBAC83B2C038D849FDE6382
SHA-256:	D0DA793571AA99C98E2AFCA3BE0F3D6850AABBACF2ACA4EEAB8013E4EBF77A67
SHA-512:	8ECD3FE32528D30C76C47763DB6723CD69D2D8842FEFCC7B3F12599B4F4F546C5AD4BD5C3C604F666FDE36FD168945303414D54CD709DF56FE96D08BBFE063 2
Malicious:	false
Reputation:	low
Preview:	.^V.e..s...^.....[K..*#..o..5.~.._..H.....;..-.$.%.O.F....24.....K.wZ.J....R;...(....)3;J.....U.*....rS...=.....}.8H7..i..I.V...DNP#.....UNzq]...I..mw...F.....Ip.K.L..z....`K._x.E.f....\|\|..6(SEG ....#.yI=.....x.^K.^.t..P.d.....\~0..:^2.B:..;EIBe.....BO.o\[.M.uM5.z..~.._..H.....;..-.j.%.O.F....2~.PR..yKR.X.....}..r}.....w.hG.B&..fW...=..Gb.;.K_E..}.8H76.....By.3.*.,k..]\| ..f.). .\ ..)..<8..Eh>x.SgFL..z.....&qx.Ep.....\|r?k.(.EG.....[h..6..4xn.^K.^.t.F...d.....T.\~s..p^2.?:.q;.IBe.....BO.G.[..uM5.>.5.~.._..H.....;..-.$.%.O.F....2~.PR..yKR.X.....}..r}. .....w.hG.B&..fW...=..Gb.;.K_E..}.8H76.....By.3.*.,k..]|..f.). .\ ..)..<8..Eh>x.SgFL..z....`K._x.E.....|r.t.(SEG.....[h..6..4xx.^K.^.t.F...d.....T.\~s..p^2.?:.q;.IBe.....BO.G.[..uM5.>. 5.~.._..H.....;..-.$.%.O.F....2~.PR..yKR.X.....}..r}.....w.hG.B&..fW...=..Gb.;.K_E..}.8H76.....By.3.*.,k..]|..f.). .\ ..)..<8..Eh>x.SgFL..z....`K._x.E.....|r.t.(SEG.....[h..6..4xx. ^K.^.t.

C:\Users\user\AppData\Local\Temp\rysgtozci.exe

Process:	C:\Users\user\Desktop\Ay9xkK3NYN.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.524680277533852
Encrypted:	false
SSDEEP:	96:X5xApGY3bxCrq+M7sYx+MeBZtXIpXSdOWPmoynsx:X5xAQY3w2QweBZVIpidPPmoyn
MD5:	96B3C3B0F05B4CEDF349797D7CB05627
SHA1:	B2D7084DCAE06676C21D0AB393C60D6480E1D03F
SHA-256:	874F73E26734628599 67AFC64C3C33C1957D7B69915124CCA91CED26DCFCD5C0
SHA-512:	E264E979679A7DCD410B2916EC16F8333CBA6A45D59FAAD99C9A45FF75D0E574D6ECBB52FB21A7B89732A8236B5F5416FD8FCFFB595692F451DD6556B9641E 3
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.1..m_B.m_B.m_B.r[B.m_B.qQB.m_B.rUB.m_BK.^C.m_B.m^B]m_B.3[C.m_B.3.B.m_B.3]C.m_BRich.m_B.....PE..L...V0sb..... ....@.....P.....".....@.....!..... ....`.....text...z..... ..`.rdata..... .....@..@.data...<....0.....@....rsrc.....@.....@..@..... ....

C:\Users\user\AppData\Local\Temp\wduqqtzg

Process:	C:\Users\user\Desktop\Ay9xkK3NYN.exe
File Type:	data
Category:	dropped
Size (bytes):	5381
Entropy (8bit):	6.0977076898399645
Encrypted:	false
SSDEEP:	96:R9mon8+8wowi4vsVmHxXTR9yprcP4b0hHryNB+3Oc02rv5FJ2EZdrH:browmYXT36r1YuIFBrv5FJXLrH
MD5:	CEA27FDA9443DD5882439188C2494A7B
SHA1:	89B7F9C46C4462F37EE6E91D639CCDD3084E03CD
SHA-256:	26A0EF0FE1FDAB9E6DAE3CAECEC085C3800A44D32CD5B87C182C0C0A6B559F59
SHA-512:	12040C4009E23EC2D4CF15A9F5B31587070F6086F2816EFEB946A6D2F1609339BA66A8639F187D2AC97D0284264DF7AEE0F62B40EA550567B5E35F66992A1C87
Malicious:	false
Preview:	;.??D.#.#.JMV.T/?.V...._.V....'.T7?..3.???.T+?>..>....7O'2???....D.>..>....7O']???....D.>..>....7O'.???....D.>..>....7O's???....D{...;....W..::...._.D[..';....'.<#..'.<3.;x...P6(..':D3.;... 3VM.T+.[/..'????.;..4..T3>..P>..Y>...W>...P>._.>.'U.-...G..6.G.C+..%8./>...Y..4../:T3'????...;.???.;.|..T+U.../.UR...?D.#HH.V....7...?......?.<...x..x;.D7..3...?..<..8..7.D3...?..9} .'.A??'.A??..?..>^.'.A??'MA??..?.|S..'EA??'.A??..?D.#.#.V....'..7.???.....3..7?....3}??..3...3..7G..7"['G4??.........P..?..|..K|...'...Px.?..|..K|.A..W..?..4.O..>^.'.8??O'.,>>..+". ..'O>..'I>>>..+..+?.=.T/?".../8???./...;?D.#.#..V....'..7.???.....3..7?....3}??..3...3..7G..7"['.;??.....???.....P..?..|..K|{.....Px.?..|..K|{.....P....|..K|{.....Y..:.....C.{..'...Px.A..|..K|{.4..W. .?..4.O..9}.'a???O' 3>>..+...?....'.<..8".>..>..>..>..>..'.5>>..+..+?.=.T/?".../8???./...?D.#.#...7.???..[..3..7?....3}??..3...3..7G..7"['.:??.....P..?..|[.K|'.....Px.?..|[.K|'.A..W..?. .4[O.|S..'.???O'.3>>..+".>..>..'v,>

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.887563460066861

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Ay9xkK3NYN.exe
File size:	219440
MD5:	5fc986129c3d833b1c7e5ba6ff3678bc
SHA1:	2ace6bc0488df9b8592e25be3de38e6c9a0c16da
SHA256:	d02d076842cc94fa6612b13ff0d2f77e1ff9150d22607cfe3962da4234cf4ed5
SHA512:	7f496926ea5026eda78532c001ce21e6f9f6ec4474ee995909a53f106def291cd7338072e56b29b7844ea43dc83fcd3eb6f8e36d2db5d8d5e0281059d60f9043
SSDEEP:	3072:l1NjcVVnLpPunbD0r9X/MP5LsCIVa1aP+KQ4kFHP67DzJEhShrM/joS9zAQNgOau:HNeZmQrV/MP8XXklIiheMLPztvau
TLSH:	DA2412351380C8E7D91B07305E392BA7D7B9AB366375931B139826ACBCA1391E31F794
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax

Instruction
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F512CDE74AAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F512CDE747Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0xa50	0xc00	False	0.402018229167	data	4.18462166815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x2e8	data	English	United States
RT_DIALOG	0x3b478	0x100	data	English	United States
RT_DIALOG	0x3b578	0x11c	data	English	United States
RT_DIALOG	0x3b698	0x60	data	English	United States
RT_GROUP_ICON	0x3b6f8	0x14	data	English	United States
RT_MANIFEST	0x3b710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:13:46.498192072 CEST	63538	53	192.168.2.5	8.8.8.8
May 5, 2022 08:13:46.538089991 CEST	53	63538	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 08:13:46.498192072 CEST	192.168.2.5	8.8.8.8	0x6b14	Standard query (0)	www.fortitude-tech.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 08:13:46.538089991 CEST	8.8.8.8	192.168.2.5	0x6b14	Name error (3)	www.fortitude-tech.com	none	none	A (IP address)	IN (0x0001)

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

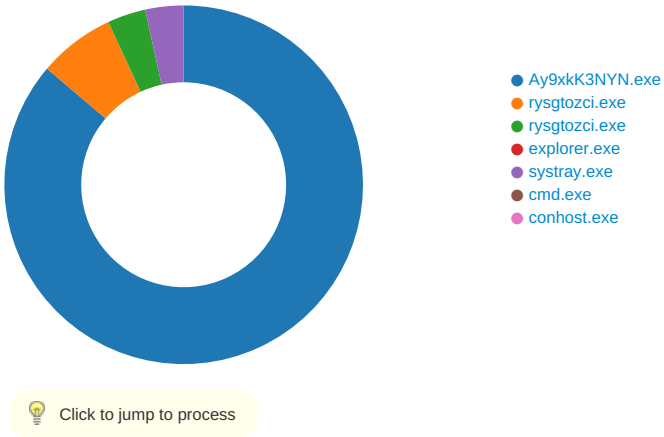
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xEA

Statistics

Behavior



System Behavior

Analysis Process: Ay9xkK3NYN.exe PID: **6376**, Parent PID: **5168**

General

Target ID:	0
Start time:	08:11:46
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\Ay9xkK3NYN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ay9xkK3NYN.exe"
Imagebase:	0x400000
File size:	219440 bytes
MD5 hash:	5FC986129C3D833B1C7E5BA6FF3678BC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: rysgtozci.exe PID: **6412**, Parent PID: **6376**

General

Target ID:	1
Start time:	08:11:48
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\rysgtozci.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\rysgtozci.exe C:\Users\user\AppData\Local\Temp\wduqqtzg
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	96B3C3B0F05B4CEDF349797D7CB05627
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: 00000001.00000002.445776431.0000000000600000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.445776431.0000000000600000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.445776431.0000000000600000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wduqqtzg	unknown	4096	success or wait	1	4011DF	fread
C:\Users\user\AppData\Local\Temp\wduqqtzg	unknown	4096	success or wait	1	4011DF	fread

Analysis Process: rysgtozci.exe PID: **6440**, Parent PID: **6412**

General

Target ID:	2
Start time:	08:11:49

Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\rysgtozci.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\rysgtozci.exe C:\Users\user\AppData\Local\Temp\wduqqtzg
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	96B3C3B0F05B4CEDF349797D7CB05627
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: 00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.553583563.00000000005E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.553285992.00000000005B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.553285992.00000000005B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.553285992.00000000005B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.441965873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.441965873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.441965873.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.440397426.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.440397426.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.440397426.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.552642858.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.552642858.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.552642858.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **6440**

General

Target ID:	3
Start time:	08:11:55
Start date:	05/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000003.00000000.491644734.000000000F6CB000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.491644734.000000000F6CB000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.491644734.000000000F6CB000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.516553688.000000000F6CB000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.516553688.000000000F6CB000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.516553688.000000000F6CB000.00000040.00000001.00040000.00000000.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: systray.exe PID: 3060, Parent PID: 684

General

Target ID:	14
Start time:	08:12:39
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xd70000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 0000000E.00000002.696256426.00000000048E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.696256426.00000000048E0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.696256426.00000000048E0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.694897544.0000000000C80000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.694897544.0000000000C80000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.694897544.0000000000C80000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.695692167.00000000048B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.695692167.00000000048B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.695692167.00000000048B0000.00000040.10000000.00040000.00000000.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	C9A457	NtReadFile

Analysis Process: cmd.exe PID: 3348, Parent PID: 3060

General

Target ID:	17

Start time:	08:12:46
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\rysgtozci.exe"
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: **6652**, Parent PID: **3348**

General

Target ID:	18
Start time:	08:12:47
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly