ID: 635291
Sample Name:
skyrunyyu655432.exe
Cookbook: default.jbs
Time: 18:34:01
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

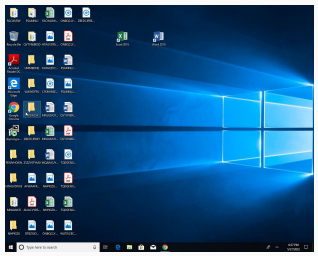
Windows Analysis Report

skyrunyyu655432.exe

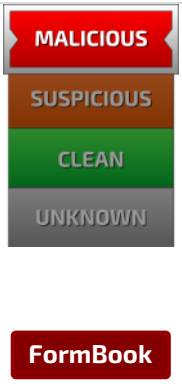
Overview

General Information

Sample Name:	skyrunyyu655432.exe
Analysis ID:	635291
MD5:	070a940ccbc84f…
SHA1:	b6624708fa177d..
SHA256:	a734d235386d77.
Tags:	exe Formbook
Infos:	



Detection



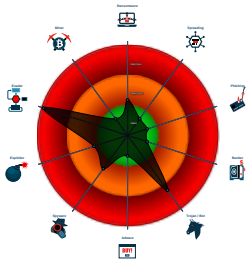
FormBook

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…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Modifies the prolog of user mode fun…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- skyrunyyu655432.exe (PID: 6220 cmdline: "C:\Users\user\Desktop\skyrunyyu655432.exe" MD5: 070A940CCBC84F85A8BA749ECCF55618)
  - jfotlqeoqb.exe (PID: 6364 cmdline: C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe C:\Users\user\AppData\Local\Temp\pvrclmgpss MD5: E85BB68B7CBEFADF0D1ACD4B7B8BD528)
    - jfotlqeoqb.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe C:\Users\user\AppData\Local\Temp\pvrclmgpss MD5: E85BB68B7CBEFADF0D1ACD4B7B8BD528)
      - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - ipconfig.exe (PID: 4108 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
          - cmd.exe (PID: 4468 cmdline: /c del "C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 3376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.boxberry-my.com/sn31/"
  ],
  "decoy": [
    "matsuomatsuo.com",
    "104wn.com",
    "bolacorner.com",
    "dawonderer.com",
    "yourpamlano.xyz",
    "mtzmx.icu",
    "lepakzaparket.com",
    "barmagli.com",
    "danta.ltd",
    "marumaru240.com",
    "people-centeredhr.com",
    "test-brew-inc.com",
    "clairvoyantbusinesscoach.com",
    "aforeignexchangeblog.com",
    "erentekbilisim.com",
    "gangqinqu123.net",
    "defiguaranteebonds.com",
    "thegioigaubong97.site",
    "vaoiwin.info",
    "vcwholeness.com",
    "03c3twpfee5estjovfu2655.com",
    "mutantapeyachtclubtoken.store",
    "pixelkev.xyz",
    "corporacioncymaz.com",
    "iampro-found.com",
    "azureconsults.com",
    "bam-bong.com",
    "advanceresubeopene.biz",
    "tzjisheng.com",
    "krdz28.online",
    "ycw2009.com",
    "minioe.com",
    "dronelink.xyz",
    "autu.cfd",
    "sdwmkj.com",
    "uixray.xyz",
    "informacion-numero-24-h.site",
    "123dianyingyuan.com",
    "tj-assets.com",
    "usaservicedogregistratuon.com",
    "metagwnics.com",
    "pepeksquad2.host",
    "kc7.club",
    "yundtremark.com",
    "finance-employers.com",
    "euroglobalnews.info",
    "estudioenzetti.com",
    "rodosmail.xyz",
    "bm65.xyz",
    "bchmtn.net",
    "server4uuss.net",
    "maisonretraiteprivee.com",
    "atelierelzaaidar.com",
    "thegurlyboutique.com",
    "primobellaquartz.com",
    "jetskirentaldublin.com",
    "akmeetech.com",
    "withoutyoutube.com",
    "blackcreekwatershed.com",
    "89qp52.com",
    "e3488.com",
    "vote4menk.com",
    "tyma.club",
    "theceditpalooza.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.292821127.0000000001660000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.292821127.0000000001660000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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
3.0.jfotlqeoqb.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.jfotlqeoqb.exe.400000.9.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.jfotlqeoqb.exe.400000.9.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$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
3.0.jfotlqeoqb.exe.400000.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.0.jfotlqeoqb.exe.400000.9.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

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 66.235.200.147

Timestamp:	192.168.2.366.235.200.14749755802031412 05/27/22-18:36:55.446707
SID:	2031412
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 66.235.200.147

Timestamp:	192.168.2.366.235.200.14749755802031453 05/27/22-18:36:55.446707
SID:	2031453
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 66.235.200.147

Timestamp:	192.168.2.366.235.200.14749755802031449 05/27/22-18:36:55.446707
SID:	2031449
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

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)

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

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

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

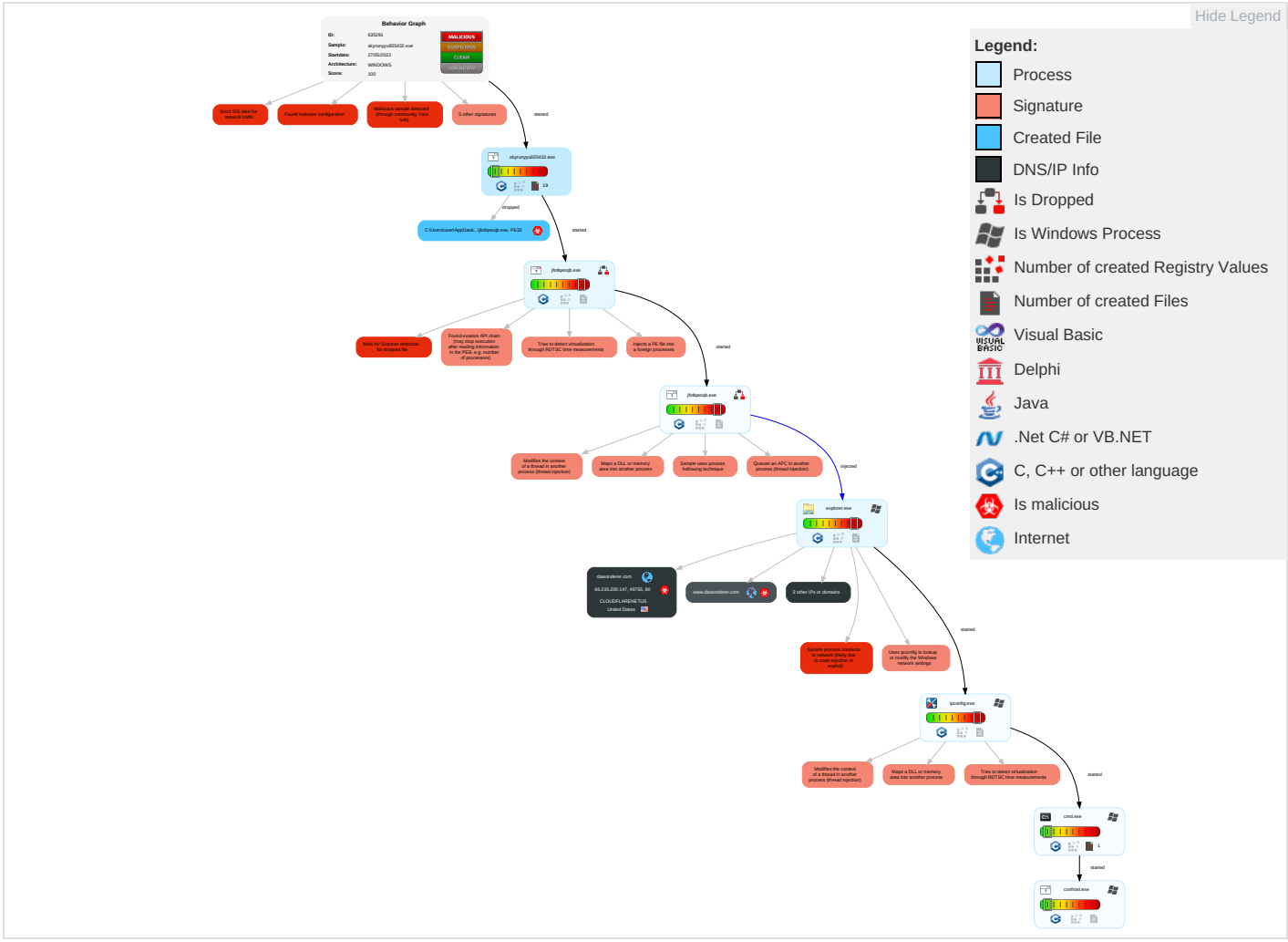
Yara detected FormBook

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

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 2 Native API	Path Interception	6 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 System Time 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	1 Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Virtualization/Sandbox Evasion	1 Input Capture	2 5 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	6 1 2 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	2 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 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	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	1 Software Packing	Cached Domain Credentials	1 System Network Configuration 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	2 File and Directory 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	Indicator Removal from Tools	Proc Filesystem	1 1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

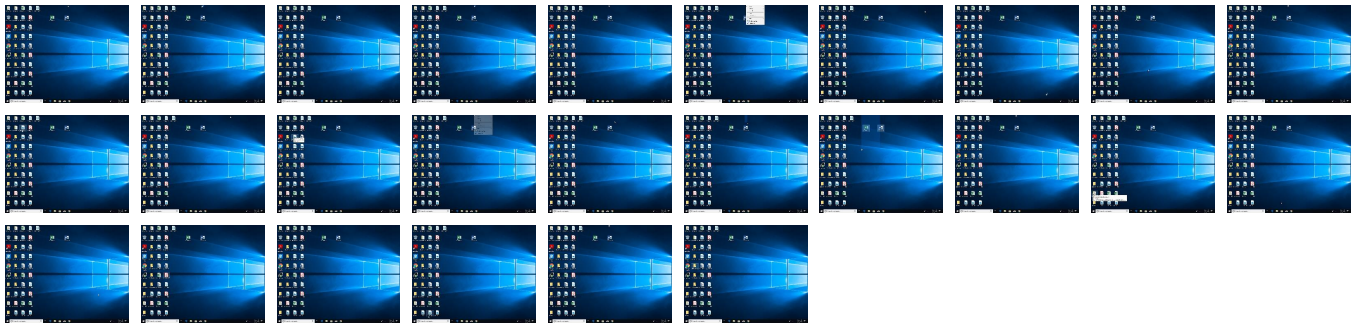
Behavior Graph



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
skyrunyyu655432.exe	42%	Virustotal		Browse
skyrunyyu655432.exe	34%	ReversingLabs	Win32.Trojan.FormBook	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe	37%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.jfotlqeoqb.exe.1660000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.jfotlqeoqb.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.jfotlqeoqb.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.jfotlqeoqb.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.jfotlqeoqb.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.boxberry-my.com/sn31/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hdr-nlb9-41371129e8304c29.elb.us-east-1.amazonaws.com	52.71.57.184	true	false		high
dawonderer.com	66.235.200.147	true	true		unknown
www.dawonderer.com	unknown	unknown	true		unknown
www.bolacorner.com	unknown	unknown	true		unknown

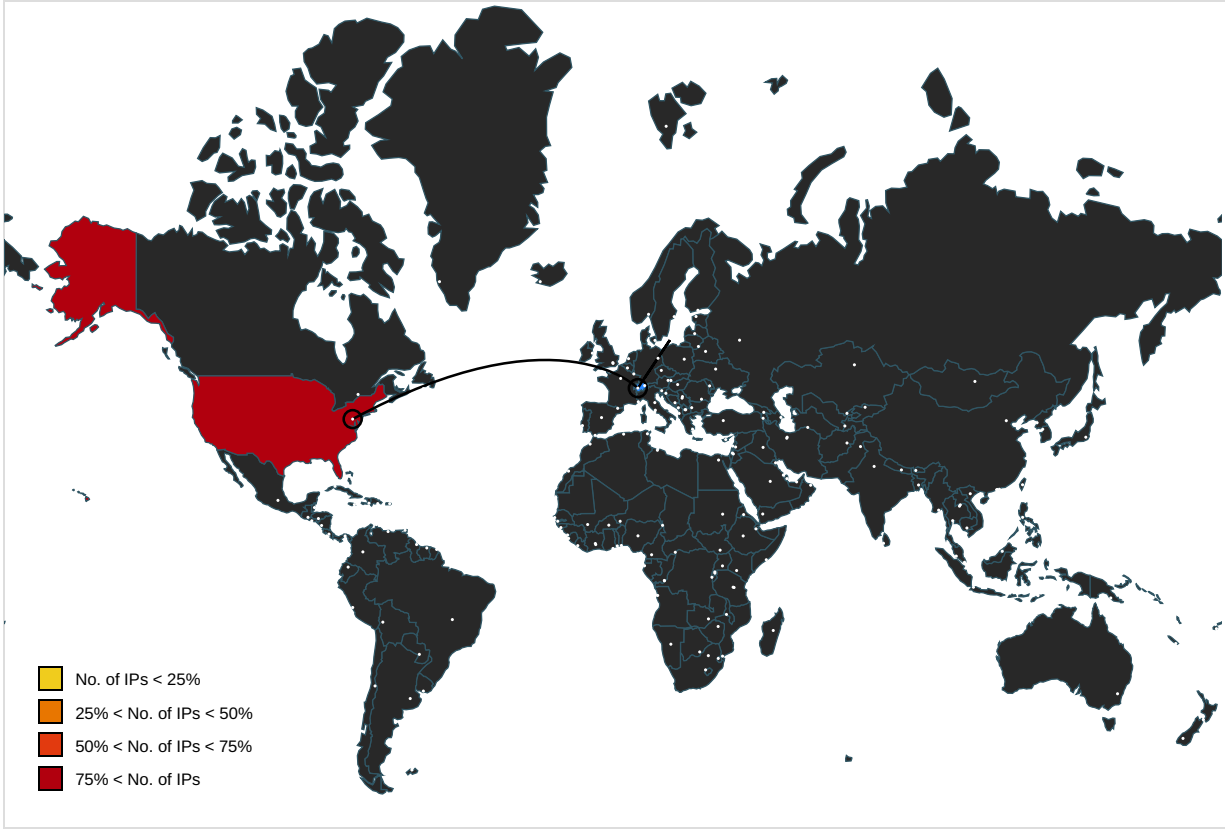
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.boxberry-my.com/sn31/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.hugedomains.com/domain_profile.cfm?d=bolacorner.com	ipconfig.exe, 0000000D.00000002.54719696.00000000035CF000.00000004.10000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.71.57.184	hdr-nlb9-41371129e8304c29.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
66.235.200.147	dawonderer.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635291
Start date and time: 27/05/202218:34:01	2022-05-27 18:34:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	skyrunyyu655432.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/4@2/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 58.7% (good quality ratio 53.8%) • Quality average: 73.1% • Quality standard deviation: 31.5%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, store-images.s-microsoft.com, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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\2e29kg38w1e

Process:	C:\Users\user\Desktop\skyrunyyu655432.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.990724029974516**
Encrypted:	**true**
SSDEEP:	3072:df6pBR3Wqc50keMwga+5HZsjYyOWdWRtFgR/r5OKOgYRsh:dCIqG0HM6aHZszOWdaFw/r59Ojsh
MD5:	83D312E5E420E4BD50B6C4439A68C9DF
SHA1:	19EC197E9059CF609F9C8279974A8C114C0F1DE9

SHA-256:	9749AACEAF7D57AA02FFE602524DAE4BF33B9A2D4EE5E814AC668A5D145E128E
SHA-512:	0101859052ADBB1E10DF3F57E627160C8AB325FD5C199D3F7D3568EE7F18CA3F1F013C793D9BBFEDB87183B670855069048CFAE1930562DDD40ACF021B853F7
Malicious:	false
Reputation:	low
Preview:	.p..*...&....N.SNd(....b..o.f.1/U.5.r...VT.G9C....0V.d\...h.Eq.....ih.d..gk..v6...4<.@....M.H...|.S.A..\....0 ...4...C.RH.0F.C..,.)y...pm.....+...C\E..w.q..*kf..i.5...ml.....G(.x[..W..k...S ..Z...M..ua...p.|.....p9.kGOK73.._..'.............3%........e..J...k..._.ku.....NUU...r..VT.G9n....0VE.d\...h.Eq..........$...7pw0$....P..ko.6..."..".."[[_....zb........RH.0F.........=7!3........X> (.kE.....$*../..:...+.6L....G(.x.......6.^.W.......M..ua.$...X.....B.kGOK73...w....C....x...3m.......&e..J...k..._.ku.....1/U.5.r...VT.G9C....0V.d\...h.Eq..........$...7pw0$....P..ko.6..."..".. [[_....zb........RH.0F.........=7!3........X>(.kE.....$*../..:...+.6L....G(.x[..W.....^oW...v...M..ua.$...X.....9.kGOK73...w....C....x...3m.......&e..J...k..._.ku.....1/U.5.r...VT.G9C....0V. d\...h.Eq..........$...7pw0$....P..ko.6..."..".."[[_....zb........RH.0F.........=7!3........X>(.kE.....$*../..:...+.6L....G(.x[..W.....^oW...v...M..ua.$...X.....9.kGOK73.

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

Process:	C:\Users\user\Desktop\skyrunyyu655432.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134144
Entropy (8bit):	6.4123316660425616
Encrypted:	false
SSDEEP:	1536:RcTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1Oy9f6zqjzswa+98qSIJnXSe:5fbnR6BqNvncvhwiz2swteq4iG5sCq
MD5:	E85BB68B7CBEFADF0D1ACD4B7B8BD528
SHA1:	6260AB4FE9793DE221C38E2785EE011178492891
SHA-256:	D4286A555EF8679CFCB40ADE56C210469C749EC48718E84FBFEA3B472825518B
SHA-512:	5011822C9BDF7F64E2AD2921D1AD15722AA2C6109BC5FB1C5115928D8057949FFCECD79E408A8731E9B4527795494E367DA7B70112360EA529F1BAD107175310
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 37%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(.}c{.}c{.}c{./.{.}c{./.{.}c{./.{.}c{(.bz.}c{.}b{.}c{y.gz.}c{y..{.}c{ y.az.}c{Rich.}c{.....PE..L...s..b.....@.....`.....@.....@.....P.....T..... ....@.....text...5..... ..`.rdata..>N.....P.....@..@.data....1.....@....rsrc.....@.....@..@.reloc.....P..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\nspF162.tmp

Process:	C:\Users\user\Desktop\skyrunyyu655432.exe
File Type:	data
Category:	dropped
Size (bytes):	334550
Entropy (8bit):	7.528668807103741
Encrypted:	false
SSDEEP:	6144:w/CIqG0HM6aHZszOWdaFw/r59OjsepvncWHsSGw:xNza5gzuoIcWHsS
MD5:	BDB87446E9230A4B38ACB065FD1A9368
SHA1:	99B36BFF00A3DC4D17E232E6D5EAFC56D387104A
SHA-256:	23140E1941470A9F0A5A2866DE11B9F406AA4C2A2CC1FED10DE02A2FE8992F77
SHA-512:	6EB8D2605E7CE5EF6A3CECE02FFBA33C863C74B2384F38B476EFF1B91F7E41658CD8BAC862D46117823443B562296A7685894ED717DC87D4C8439C90F0BE894 6
Malicious:	false
Reputation:	low
Preview:	I.....,.....H.....I..... .....B.....j.....]..... ....

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

Process:	C:\Users\user\Desktop\skyrunyyu655432.exe
File Type:	data
Category:	dropped
Size (bytes):	4734
Entropy (8bit):	6.200882416738238
Encrypted:	false
SSDEEP:	96:JATyzXT6CUhlueeyfioCBRFAfgbMRE5jBL8q5y55m0Y:JATy3VveoBoFAfgb6wFqk
MD5:	15004B2E0FE7FC55E5E6FBFACF737244
SHA1:	509F67F7A859512E9964D9AA9EC38329AF4C2B6A
SHA-256:	24051CD359262971B696AD209D9A66C43221A389C56B7324B7FA4D2DF7DB5C00

SHA-512:	71BF196170FFDE6C22E0E39759891709B7947D5332BE5E5EDEFD97B2AFA1CA301FEEFBC9BFBE817FC6EF1726BBB0DF97B66B3075C08093825823841546C0014F
Malicious:	false
Preview:	.....L~...l..L~...d..t.E.....t.d.....T..`.....t.d.....\..h.....t.dS.....D..P.....t.d@.....L..X.....z..qL...+..l.....d..[..d.....d....C.Rz..u...d....B.....z.d.....8.Q1....T..\ ..D...L...l..d.....u.....T.....d....E.8.9.....8.Q.....[B.....L~...t.....C..C...t.....t..[B...^.dr...d..B...~.m.d..d..B....!.d...d...B.....L~...dE.t.....T....t.....^.....t...t..d....L....+z..q[...T..`..d+z..Cc...T..`z.z..qL...T..~.m.dQ....dR.....d...d.....E.....[B.....L~...dE.t.....L....t.....^.....t...t..d+....L.....+z..q[...L..X..+z..Cc...L..X..+z..Sc..L..X...[z..qR...L..X..d+z..Cc...L..Xz.z..qL...L..^.db....d.....d.....d.....E.....[B.....E.t.....t.....^.....t...t..d"....L....+z..q[.....d..+z..Cc.....dz.z..qL.....!.d?....d0.....d5..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.939796551575706
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	skyrunyyu655432.exe
File size:	278102
MD5:	070a940ccbc84f85a8ba749eccf55618
SHA1:	b6624708fa177d6a591c01ba291d40390bb6d8e7
SHA256:	a734d235386d77a1c6a88bdf63efce5134a82a90e113be647200401b717b891e
SHA512:	5bcd64f98431c61774901e6fd0dca10e39634ba52b122d4362df8f335ba30f70e6ccf04dacef9af2af1b1a5351d2d27b279ce87c1a92783478c2534502ea69cb
SSDEEP:	6144:B0Ykc3Mje3wl1Xv3pXF0E3/eIZpg63Zb73lUWeboQXJKAw2mttww:0Gyzl1/3HeItJVUWulQAw2rw
TLSH:	504412D337E2C1EBD4070A315F7665B2F371A268932B52C70BA05F2A6F711CAD912296
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qJ...$...$...$./. {...$...%.;.$.".y...$..3....$.f."...$.Rich..$.....PE..L.....iF.....Z.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4032fa
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:	
Time Stamp:	0x4669CEB6 [Fri Jun 8 21:48:38 2007 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:	55f3dfd13c0557d3e32bcbc604441dd3

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx

Instruction
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409170h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push ebx
call dword ptr [00407278h]
mov dword ptr [00423FD4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F4E8h
call dword ptr [00407154h]
push 0040922Ch
push 00423720h
call 00007F3D90DA7A58h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007F3D90DA7A46h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007F3D90DA52BCh
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F3D90DA7539h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007F3D90DA5315h
cmp cl, 00000020h
jne 00007F3D90DA52B8h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F3D90DA52ACh
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007F3D90DA52B8h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007F3D90DA52E5h
inc eax
cmp byte ptr [eax], 00000053h
jne 00007F3D90DA52C0h

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	0x73a0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	0x7000	0x288	.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	0x59ac	0x5a00	False	0.668142361111	data	6.45807821776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x117a	0x1200	False	0.4453125	data	5.17513527374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1afd8	0x400	False	0.6015625	data	4.98110806401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94448786242	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, CreateFileA, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, CloseHandle, ExitProcess, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

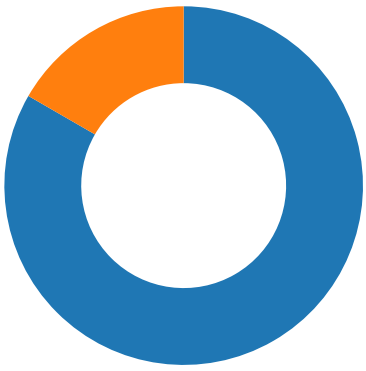
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.366.235.200.147475580203141205/27/22-18:36:55.446707	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.3	66.235.200.147
192.168.2.366.235.200.147475580203145305/27/22-18:36:55.446707	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.3	66.235.200.147
192.168.2.366.235.200.147475580203144905/27/22-18:36:55.446707	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.3	66.235.200.147

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:36:55.291124105 CEST	49755	80	192.168.2.3	66.235.200.147
May 27, 2022 18:36:55.308113098 CEST	80	49755	66.235.200.147	192.168.2.3
May 27, 2022 18:36:55.308240891 CEST	49755	80	192.168.2.3	66.235.200.147
May 27, 2022 18:36:55.446707010 CEST	49755	80	192.168.2.3	66.235.200.147
May 27, 2022 18:36:55.463802099 CEST	80	49755	66.235.200.147	192.168.2.3
May 27, 2022 18:36:55.949002028 CEST	49755	80	192.168.2.3	66.235.200.147
May 27, 2022 18:36:55.968122005 CEST	80	49755	66.235.200.147	192.168.2.3
May 27, 2022 18:36:55.968209028 CEST	49755	80	192.168.2.3	66.235.200.147
May 27, 2022 18:37:16.683904886 CEST	49762	80	192.168.2.3	52.71.57.184
May 27, 2022 18:37:16.821118116 CEST	80	49762	52.71.57.184	192.168.2.3
May 27, 2022 18:37:16.821217060 CEST	49762	80	192.168.2.3	52.71.57.184
May 27, 2022 18:37:16.821484089 CEST	49762	80	192.168.2.3	52.71.57.184
May 27, 2022 18:37:16.958137035 CEST	80	49762	52.71.57.184	192.168.2.3
May 27, 2022 18:37:16.958177090 CEST	80	49762	52.71.57.184	192.168.2.3
May 27, 2022 18:37:16.958417892 CEST	49762	80	192.168.2.3	52.71.57.184
May 27, 2022 18:37:16.958487034 CEST	49762	80	192.168.2.3	52.71.57.184
May 27, 2022 18:37:17.094350100 CEST	80	49762	52.71.57.184	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:36:54.274760008 CEST	49873	53	192.168.2.3	8.8.8.8
May 27, 2022 18:36:54.414109945 CEST	53	49873	8.8.8.8	192.168.2.3
May 27, 2022 18:37:16.569818974 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 18:37:16.679555893 CEST	53	65266	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:36:54.274760008 CEST	192.168.2.3	8.8.8.8	0x62ef	Standard query (0)	www.dawonderer.com	A (IP address)	IN (0x0001)
May 27, 2022 18:37:16.569818974 CEST	192.168.2.3	8.8.8.8	0x79c2	Standard query (0)	www.bolacorner.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:36:54.414109945 CEST	8.8.8.8	192.168.2.3	0x62ef	No error (0)	www.dawonderer.com	dawonderer.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:36:54.414109945 CEST	8.8.8.8	192.168.2.3	0x62ef	No error (0)	dawonderer.com		66.235.200.147	A (IP address)	IN (0x0001)
May 27, 2022 18:37:16.679555893 CEST	8.8.8.8	192.168.2.3	0x79c2	No error (0)	www.bolacorner.com	traff-1.hugedomains.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:37:16.679555893 CEST	8.8.8.8	192.168.2.3	0x79c2	No error (0)	traff-1.hugedomains.com	hdr-nlb9-41371129e8304c29.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:37:16.679555893 CEST	8.8.8.8	192.168.2.3	0x79c2	No error (0)	hdr-nlb9-41371129e8304c29.elb.us-east-1.amazonaws.com		52.71.57.184	A (IP address)	IN (0x0001)
May 27, 2022 18:37:16.679555893 CEST	8.8.8.8	192.168.2.3	0x79c2	No error (0)	hdr-nlb9-41371129e8304c29.elb.us-east-1.amazonaws.com		54.209.32.212	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dawonderer.com
- www.bolacorner.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49755	66.235.200.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:36:55.446707010 CEST	1233	OUT	GET /sn31/?m6R01xM0=qZl/JLX84vnD5ytzVzk0/a0Hcpketn5qZPO1CaBkWF6tW2qs6ow5h/A/zRQwl5G72f7o&n PqD=gvLpMpxpWl HTTP/1.1 Host: www.dawonderer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49762	52.71.57.184	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:37:16.821484089 CEST	9605	OUT	GET /sn31/?m6R01xM0=f82GdrL9BOGPadRnOYEWsPSt+bOR3tUYa+dCVqOhmg/09rEzcw7t3bM5PuUufbFtM3zx&n PqD=gvLpMpxpWl HTTP/1.1 Host: www.bolacorner.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:37:16.958137035 CEST	9605	IN	HTTP/1.1 302 Found content-length: 0 date: Fri, 27 May 2022 16:37:15 GMT location: https://www.hugedomains.com/domain_profile.cfm?d=bolacorner.com connection: close

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

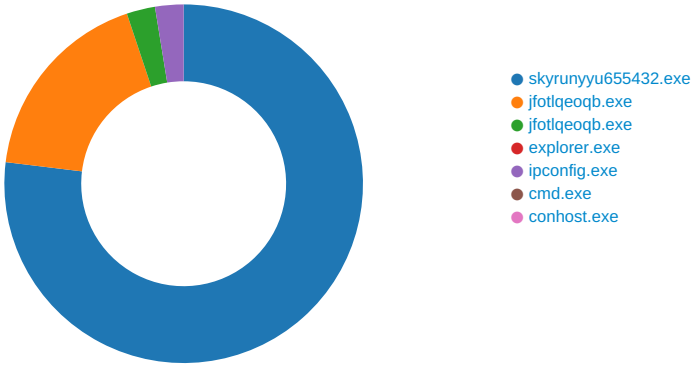
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8C 0xCE 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x84 0x4E 0xE1

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: skyrunyyu655432.exe PID: **6220**, Parent PID: **5112**

General

Target ID:	0
Start time:	18:35:17
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\skyrunyyu655432.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\skyrunyyu655432.exe"
Imagebase:	0x400000
File size:	278102 bytes
MD5 hash:	070A940CCBC84F85A8BA749ECCF55618
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: jfotlqeoqb.exe PID: **6364**, Parent PID: **6220**

General

Target ID:	2
Start time:	18:35:19
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe C:\Users\user\AppData\Local\Temp\pvrclmgpss
Imagebase:	0x1e0000
File size:	134144 bytes
MD5 hash:	E85BB68B7CBEFADF0D1ACD4B7B8BD528
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: 00000002.00000002.292821127.0000000001660000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292821127.0000000001660000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292821127.0000000001660000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 37%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\pvrclmgpss	unknown	4096	success or wait	1	1EF88C	ReadFile
C:\Users\user\AppData\Local\Temp\pvrclmgpss	unknown	4096	success or wait	1	1EF88C	ReadFile
C:\Users\user\AppData\Local\Temp\2e29kg38w1e	unknown	189439	success or wait	1	16509ED	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	165051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	165051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	165051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	165051C	ReadFile

Analysis Process: jfotlqeoqb.exe PID: **6404**, Parent PID: **6364**

General

Target ID:	3
Start time:	18:35:20
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe C:\Users\user\AppData\Local\Temp\pvrclmgpss
Imagebase:	0x1e0000
File size:	134144 bytes
MD5 hash:	E85BB68B7CBEFADF0D1ACD4B7B8BD528
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: 00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.287926712.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.372936782.0000000001850000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.372936782.0000000001850000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.372936782.0000000001850000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.290240049.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.290240049.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.290240049.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.372684561.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.372684561.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.372684561.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.372998768.00000000019A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.372998768.00000000019A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.372998768.00000000019A0000.00000040.10000000.00040000.00000000.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: **3968**, Parent PID: **6404**

General

Target ID:	6
Start time:	18:35:27
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
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: 00000006.00000000.337685693.000000000EC39000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.337685693.000000000EC39000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.337685693.000000000EC39000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.359555357.000000000EC39000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.359555357.000000000EC39000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.359555357.000000000EC39000.00000040.00000001.00040000.00000000.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: ipconfig.exe PID: **4108**, Parent PID: **3968**

General

Target ID:	13
Start time:	18:35:59
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x160000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
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: 0000000D.00000002.545200841.00000000024C0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.545200841.00000000024C0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.545200841.00000000024C0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.545564197.0000000002680000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.545564197.0000000002680000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.545564197.0000000002680000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.545372443.0000000002600000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.545372443.0000000002600000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.545372443.0000000002600000.00000040.10000000.00040000.00000000.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	24DA457	NtReadFile

Analysis Process: cmd.exe PID: **4468**, Parent PID: **4108**

General

Target ID:	14
Start time:	18:36:05
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\jfotlqeoqb.exe"
Imagebase:	0xc20000
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: **3376**, Parent PID: **4468**

General

Target ID:	15
Start time:	18:36:06
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly