ID: 635319
Sample Name: O1ySvN9SvL
Cookbook: default.jbs
Time: 19:09:02
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report O1ySvN9SvL 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 8
E-Banking Fraud 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 12
Public IPs 13
General Information 13
Warnings 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Users\user\AppData\Local\Temp\fz42030wual6detyg 14
C:\Users\user\AppData\Local\Temp\kplemx 15
C:\Users\user\AppData\Local\Temp\nsr4D4E.tmp 15
C:\Users\user\AppData\Local\Temp\zrztlh.exe 15
Static File Info 16
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Rich Headers 17
Data Directories 18
Sections 18
Resources 18
Imports 18
Possible Origin 19
Network Behavior 19
Snort IDS Alerts 19
Network Port Distribution 19
TCP Packets 20
UDP Packets 20
DNS Queries 20

Copyright Joe Security LLC 2022

DNS Answers 20
HTTP Request Dependency Graph 20
HTTP Packets 20
Code Manipulations 21
User Modules 21
Hook Summary 21
Processes 21
Statistics 21
Behavior 21
System Behavior 22
Analysis Process: O1ySvN9SvL.exePID: 6268, Parent PID: 5876 22
General 22
File Activities 22
Analysis Process: zrztlh.exePID: 5816, Parent PID: 6268 22
General 22
File Activities 22
File Read 22
Analysis Process: zrztlh.exePID: 6000, Parent PID: 5816 22
General 22
File Activities 23
File Read 23
Analysis Process: explorer.exePID: 684, Parent PID: 6000 23
General 23
File Activities 24
Analysis Process: NETSTAT.EXEPID: 6124, Parent PID: 684 24
General 24
File Activities 24
File Read 24
Analysis Process: cmd.exePID: 6396, Parent PID: 6124 24
General 24
File Activities 25
Analysis Process: conhost.exePID: 5704, Parent PID: 6396 25
General 25
Disassembly 25

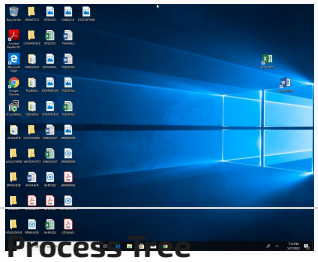
Windows Analysis Report

O1ySvN9SvL

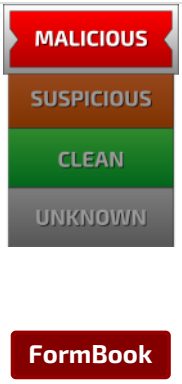
Overview

General Information

Sample Name:	O1ySvN9SvL (renamed file extension from none to exe)
Analysis ID:	635319
MD5:	caa4c5d863a932..
SHA1:	003348501064dc..
SHA256:	6796f10e7f6140f..
Tags:	32 exe Formbook trojan
Infos:	



Detection



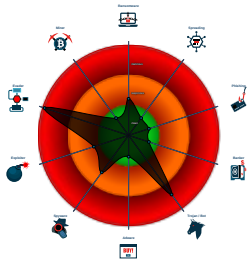
FormBook

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…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Uses netstat to query active networ…
- Maps a DLL or memory area into an…
- Modifies the prolog of user mode fun…

Classification



Process Tree

- **System is w10x64**
- O1ySvN9SvL.exe (PID: 6268 cmdline: "C:\Users\user\Desktop\O1ySvN9SvL.exe" MD5: CAA4C5D863A9324FA6B3A735ED446897)
  - zrztlh.exe (PID: 5816 cmdline: C:\Users\user\AppData\Local\Temp\zrztlh.exe C:\Users\user\AppData\Local\Temp\kplemx MD5: 917BF3E1E68704B188F2192850C76FA6)
    - zrztlh.exe (PID: 6000 cmdline: C:\Users\user\AppData\Local\Temp\zrztlh.exe C:\Users\user\AppData\Local\Temp\kplemx MD5: 917BF3E1E68704B188F2192850C76FA6)
      - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - NETSTAT.EXE (PID: 6124 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
          - cmd.exe (PID: 6396 cmdline: /c del "C:\Users\user\AppData\Local\Temp\zrztlh.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 5704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2022

```
{
  "C2 list": [
    "www.knoxvillehojo.com/a5vu/"
  ],
  "decoy": [
    "larrysormonddaytona.com",
    "stagify.net",
    "polyesterwadding.com",
    "smartcontractauditing.xyz",
    "pier88lasvegas.com",
    "albertapainters.com",
    "mujid24s.com",
    "tidyaghast.com",
    "viatempo.com",
    "gzqgc.com",
    "pragmatic168.pro",
    "gapeminimalistic.online",
    "bloomingbeauties247.com",
    "thaiperty.com",
    "thebrocab.com",
    "dinkycars.net",
    "alphamaio.com",
    "skoolksa.com",
    "kongresprawnikow.info",
    "cryptoinvestment.gold",
    "datcapark.com",
    "ashleystawart.com",
    "allure-selectshop.com",
    "uranolite.xyz",
    "zjgw88.com",
    "jimsvarietyshop.com",
    "visual-industry.com",
    "inboxburn.xyz",
    "rrew.tools",
    "denizdenobjeler.com",
    "infoshope.com",
    "50mim6.com",
    "zdcx123.com",
    "668400.com",
    "authopro.xyz",
    "techwebsite.tech",
    "bluelioninvestments.com",
    "loncheraspanama.com",
    "legalnurseresearch.net",
    "leonwarrencapital.com",
    "456837.com",
    "killercatsss.com",
    "alpha-farmers.info",
    "myoilomega.com",
    "lavid.life",
    "toxicwaterclaims.com",
    "xiaoqimz.xyz",
    "nights.life",
    "digsbury.ventures",
    "apclimo.com",
    "tinasglorybutter.com",
    "savingshk.com",
    "chanongrouptowercrane.com",
    "ugcuk.com",
    "saint-leo.com",
    "jiujiecanyin.com",
    "santamariaweddings.com",
    "mandap.xyz",
    "saigonloving.com",
    "huntingblindbrackets.com",
    "myjurorapp.com",
    "multiconnectico.com",
    "xn--oy2ay6s.xn--55qx5d",
    "businessvlogging.com"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$sqlite3step: 68 34 1C 7B E1 • 0x1892c:$sqlite3step: 68 34 1C 7B E1 • 0x18848:$sqlite3text: 68 38 2A 90 C5 • 0x1896d:$sqlite3text: 68 38 2A 90 C5 • 0x1885b:$sqlite3blob: 68 53 D8 7F 8C • 0x18983:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.532479062.00000000011E0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.532479062.00000000011E0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 • 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c8fa:$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.zrztlh.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.zrztlh.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1aaf7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bafa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.zrztlh.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a19:$sqlite3step: 68 34 1C 7B E1 • 0x17b2c:$sqlite3step: 68 34 1C 7B E1 • 0x17a48:$sqlite3text: 68 38 2A 90 C5 • 0x17b6d:$sqlite3text: 68 38 2A 90 C5 • 0x17a5b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b83:$sqlite3blob: 68 53 D8 7F 8C
2.0.zrztlh.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
2.0.zrztlh.exe.400000.8.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:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b8f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF 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: 192.168.2.5 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.5188.114.97.349798802031449 05/27/22-19:11:52.547625
SID:	2031449
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.5188.114.97.349798802031412 05/27/22-19:11:52.547625
SID:	2031412
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.5188.114.97.349798802031453 05/27/22-19:11:52.547625
SID:	2031453
Source Port:	49798
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

Copyright Joe Security LLC 2022

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

Uses netstat to query active network connections and open ports

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

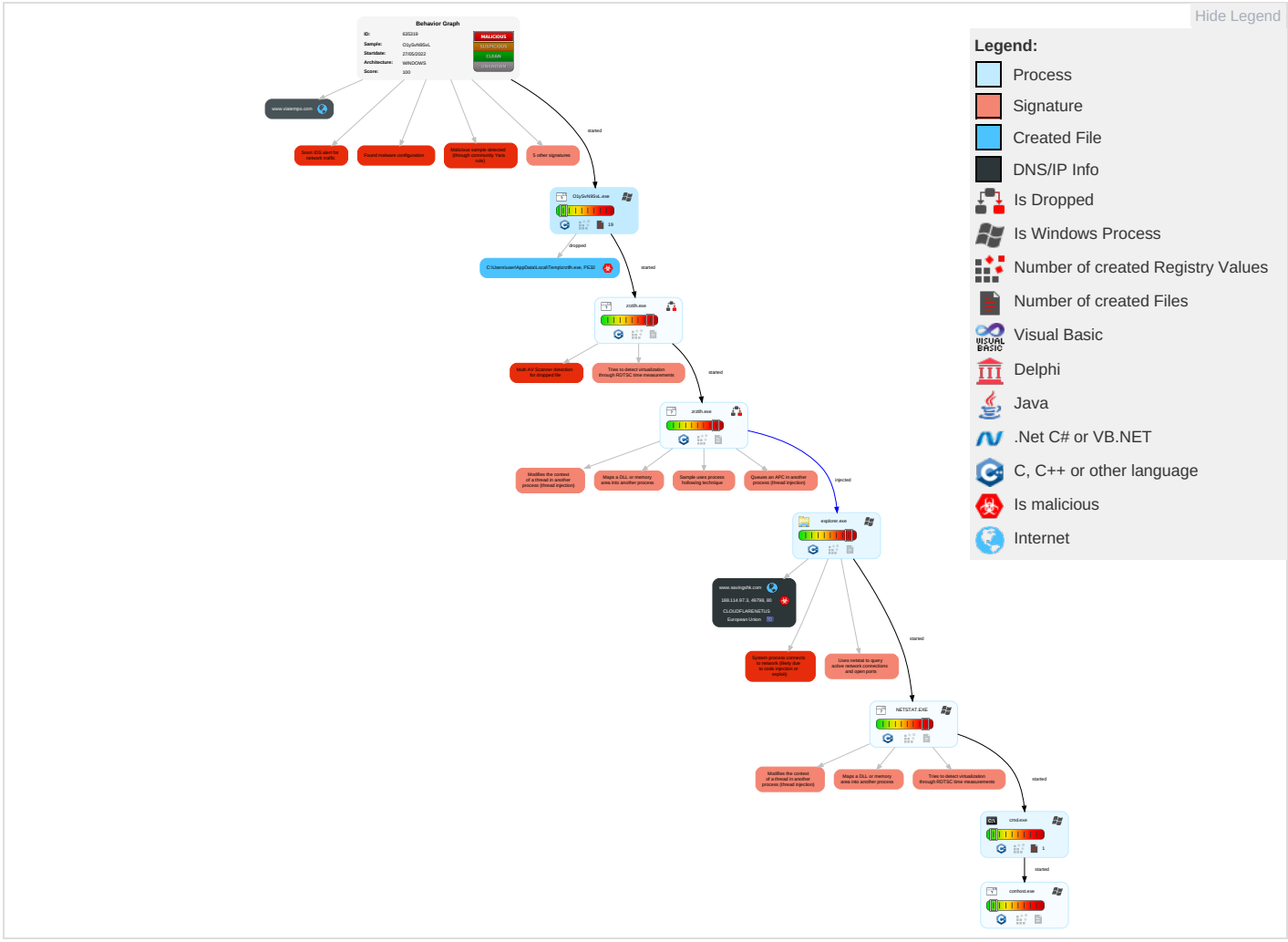
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	Path Interception	5 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	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	3 Obfuscated Files or Information	1 Input Capture	1 System Network Connections Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	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 Rootkit	NTDS	1 2 3 System Information 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	2 Virtualization/Sandbox Evasion	LSA Secrets	2 5 1 Security Software 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	5 1 2 Process Injection	Cached Domain Credentials	2 Virtualization/Sandbox Evasion	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 Process 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 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

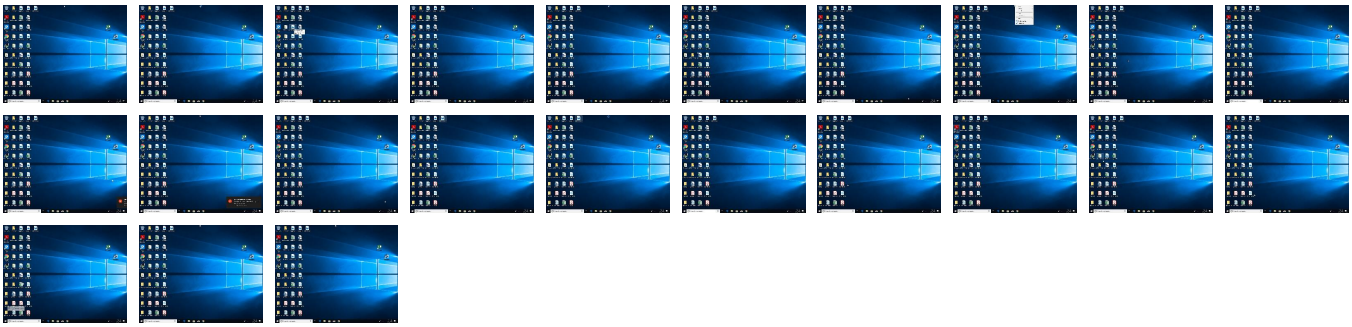
Copyright Joe Security LLC 2022



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
O1ySvN9SvL.exe	49%	Virustotal		Browse
O1ySvN9SvL.exe	54%	ReversingLabs	Win32.Trojan.GenericML	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\zrztlh.exe	50%	ReversingLabs	Win32.Trojan.GenericML	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.zrztlh.exe.730000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.zrztlh.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.zrztlh.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.zrztlh.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
2.0.zrztlh.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.savingshk.com/a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3Sf9IrYXmxrDB/U5IQUf	0%	Avira URL Cloud	safe	
www.knoxvillehojo.com/a5vu/	100%	Avira URL Cloud	malware	
http://https://www.savingshk.com/a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3S	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.viatempo.com	216.120.146.201	true	false		unknown
www.savingshk.com	188.114.97.3	true	true		unknown

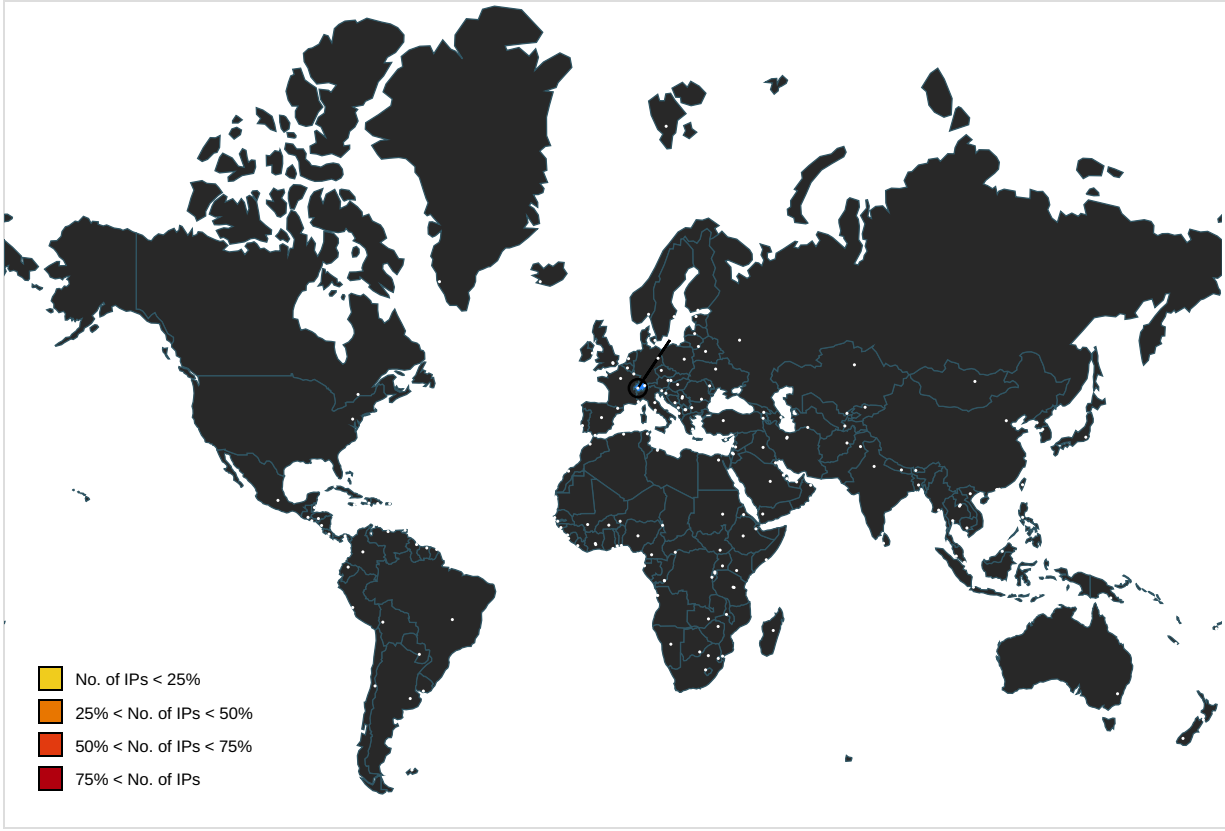
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.savingshk.com/a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3Sf9IrYXmxrDB/U5IQUf	true	• Avira URL Cloud: safe	unknown
www.knoxvillehojo.com/a5vu/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.savingshk.com/a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3S	NETSTAT.EXE, 0000000A.00000002.719201108.0000000003D4F000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.97.3	www.savingshk.com	European Union		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635319
Start date and time: 27/05/202219:09:02	2022-05-27 19:09:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	O1ySvN9SvL (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@9/4@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 58.8% (good quality ratio 55%) • Quality average: 75.6% • Quality standard deviation: 30.2%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.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\fz42030wual6detyg

Process:	C:\Users\user\Desktop\O1ySvN9SvL.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.990543351142842**
Encrypted:	**true**
SSDEEP:	3072:3W8NRWCc/+Y9Mo9Cvaa0i2De04Di8mFKybyGTqdm4GeHI/ynYyK5HXzK0ZX:G8jWaY9rSEin0aYHl7eHsyvizKUX
MD5:	2F03137B6ADB6A4BA50A0A014B8FCF5B
SHA1:	0A5753B7E38D9DBCCC0FCAED140DDDC90EFC0E1B
SHA-256:	1BF030BEE594672626E0855BFBCCDAA99803A12ABCED6B47F079B8C5BAFF8D88
SHA-512:	701CC2857B61D2FB70CE7556BC53B7C45055C1382AE3E288A76307AED77F84DE1C58F93FCD0865334F766F835D7862766CE93105E5E79BE64F161B295E353996
Malicious:	false

Reputation:	low
Preview:	.].P.U&G.7.S)B1ld.w0...9..4..d.O.9u....`.3.%.....~..t.!e1~..08Z....{...gHp.E..#Q.{...8er_R}.G....\U....Iv....U8l.....!..c.=~.G....VF.....&U..{P.....+.... ....uY8.*.....^.g.*.41.....v .K.Bn1./R...&...../Z.Hc..36n.@...n.U..C..?..+..Axwj.....U&G.....N..f..0..6[..R.S....d)O..u..."`...%....Q..~..t..e1~-/@eZ.lqp..1.....@y.d~.(...E..\.[v.B.|...AR.H.....n.7.....!..$..g..Bk=. .`2E...q5....Pgz..s8g.6C.....d~.....^.g.*...KW...."...(....U.n../R...h....sU/.X.?..36n.@.:..n....C@..?..+..AxGj.S....U&G.....N..fph0..6[..R.....d.O.9u....`.3.%.....~..t..e1~-/@e Z.lqp..1.....@y.d~.(...E..\.[v.B.|...AR.H.....n.7.....!..$..g..Bk=..`2E...q5....Pgz..s8g.6C.....d~.....^.g.*.41.....X.....,c.n1./R...h....sU/ZX.c..36n.@.:..n....C@..?..+..AxGj.S....U&G.. ...N..fph0..6[..R.....d.O.9u....`.3.%.....~..t..e1~-/@eZ.lqp..1.....@y.d~.(...E..\.[v.B.|...AR.H.....n.7.....!..$..g..Bk=..`2E...q5....Pgz..s8g.6C.....d~.....^.g.*.41.....X.....,c.n1./ R...h....sU/ZX.c..36n.@.

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

Process:	C:\Users\user\Desktop\O1ySvN9SvL.exe
File Type:	data
Category:	dropped
Size (bytes):	4811
Entropy (8bit):	6.195912775198777
Encrypted:	false
SSDEEP:	96:ylr2sDOhzseowSoyp4Qo7ubAMaNbULFA5s2Flqj4ONtgOhrukWrISrbBMEPOyAn:DrKtsyM4c/1MA4stgaCRcARZ6
MD5:	5A816A757CA8331C0761575182A29C6A
SHA1:	23C2F53AC662791B9C8594FC7F95D383EC850BFF
SHA-256:	0383B4CF1FFA4FCC73FD47A22FCC3B6E6F3A57F7F5DF8782EC6074325131C501
SHA-512:	7422469246BE9836F82CB6E42764D8332C2506B1C965D5753CD3272ECD8406BDB0AFA28F0A835AD55E7C299C90D8DDC82B54E5253A447418BE4973CE482C468
Malicious:	false
Reputation:	low
Preview:	uRVNN..z.z.....^NW...W;.nW...W;.v..fN..j6NNN..bNg.Zg.>..f.vcNNN.....g.Zg.>..f.vpNNN..~...g.Zg.>..f.v}NNN.....g.Zg.>..f.v.NNN.....>R.$.V..KK.Z...n..r..>.vR....v..z.. v..j.R..|.>._]..vK.j.R...j....b.r^..vNNNN.R2Q.3.jg..g.~.g...g...g.n.g.v..`.>...Z_....b..xM.^g.....VWQ..^K.jvNNNN..2R+NNN.R2Y...b....^.....ZN..z..W...W;.f..V.N#.Z....V.N..>.B....R.. f..j..V.N...V.M..f.j..ZN.@d..v.LNNv.LNN.BN..g..v.LNNv.LNN.VN.Y...v.LNNv.LNN.VN..z.z6W...W;.v..f>NNN.....j..fN.@..j.NN..j...j..f...fsrv.QNN.....V..V..N..Y...Y...v..V..mN. .Y...Y..L.V..N..Q....g..v.MNN.v|igg..bsW..v.g.Vv.ggg..b..bN.P..^NsO..^MNNN..^..RN..z.z.W...W;.v..f6NNN.....j..fN.@..j.NN..j...j..f...fsrv.RNN.W..NNN..V..V..N..Y...Y...Z.. V..mN..Y...Y...>..V.}m..Y...Y...B...V..|K..A...A...v..V..mL..Y...Y..Q.V..N..Q...@d..vlNNN.vujgg..b..FN.V..v..F.Ms?g.Fg.Bg.>g.Zg.Vv%hgg..b..bN.P..^NsO..^MNNN..^..BN..z.zJ. .f>NNN..r..j..fN.@..j.NN..j...j..f...fsrv.KNN.....V..V..N..Yr..Yv..Z..V..mN..Yr..Yv.L.V..N..Qr..Y...v1NNN.v:jgg..bsXg.Zg.Vv.ig

C:\Users\user\AppData\Local\Temp\nsr4D4E.tmp

Process:	C:\Users\user\Desktop\O1ySvN9SvL.exe
File Type:	SysEx File - SIEL
Category:	dropped
Size (bytes):	394442
Entropy (8bit):	7.43868018426752
Encrypted:	false
SSDEEP:	6144:/C8jWaY9rSEin0aYHl7eHsyvizKUhxpvncW10o4at3+9:BxY9rS1n0fFq1a+URcW1IaY9
MD5:	5F2A84C4D87AE80B1D56277924271C6B
SHA1:	BF341A6B52F2B69D350AC231E00E7B44224FED0D
SHA-256:	4D361A619A510FC283CDA3C34893C71D1D6B0C0D5F54DBBA246B0D6D893FF51D
SHA-512:	A21DD4791565DE12CDA5BDFEEFC726D51E7C5490AC5C6CD3F8A707F985D925AF316114B1EC1112B8D3E0D302B4692217C9F9FBC5E918D3B08505781F54DDFF BE
Malicious:	false
Reputation:	low
Preview:	.!.....,.....n.....!.....!..... .....B.....j.....N..... ....

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

Process:	C:\Users\user\Desktop\O1ySvN9SvL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	191488
Entropy (8bit):	6.542039769461921
Encrypted:	false
SSDEEP:	3072:qfbnR6BqNvncvhwE8H0o45It38FSDblJpekds39:cpvncW10o4at3+9
MD5:	917BF3E1E68704B188F2192850C76FA6
SHA1:	9AFF83C33B7D35925C4F99075B6659EF9CBE23E0
SHA-256:	D5DF78D10BA5FD20DF7A5F27EE16146FC49842D2CD1FB6FDB94C3ABFF41DC77C
SHA-512:	EA0AD1985F6289DECA99221B6248050F91A7144884805D899E147FD561C931B6F25D9FD3DA290877AA9A37A1DFD67494998CB16B6D1BD0D8475C71422D0E8FB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%

Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z..4...4...4.....4....4.....4.C.5...4...5...4...0...4.....4...6...4.Rich..4.. .....PE..L.....b.....\.....p....@.....P.....@..... .....0.....(...T.....@.....p..... .....text....[.....\..... ..`.rdata..fa...p...b...`.....@..@.data...,1.....@....rsrc..... .....@..@.reloc.....0.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.946129305576003
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:	O1ySvN9SvL.exe
File size:	299086
MD5:	caa4c5d863a9324fa6b3a735ed446897
SHA1:	003348501064dc5646b19019592f8aefa4b44f5b
SHA256:	6796f10e7f6140f26a49bf9446b2c75dfe0e6dc7d7d88cad5e09d9b608107851
SHA512:	b2cdfc4617c7ba15bc75bb9c1aa03c3e26ce7b0553c6198a18f776ae723720191936f49b09167206b71e1b2daaac09e1b10009a814a3fe2d62c18b0e79e5f161
SSDEEP:	6144:B0Ym483boybmrpR0iOITP23OHYx2tF7G2vd5EtPHuwQOEi:q3EybmrrpTUjxyF7XvrEtPHhf
TLSH:	F25413663DE060FFF64104B30A33CB2A93775E151521A51397723FEFAC2A0DAA5263D4
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
push ebp

Instruction
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 00007FC668A9FF08h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007FC668A9FEF6h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007FC668A9D76Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007FC668A9F9E9h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007FC668A9D7C5h
cmp cl, 00000020h
jne 00007FC668A9D768h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FC668A9D75Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007FC668A9D768h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007FC668A9D795h
inc eax
cmp byte ptr [eax], 00000053h
jne 00007FC668A9D770h

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

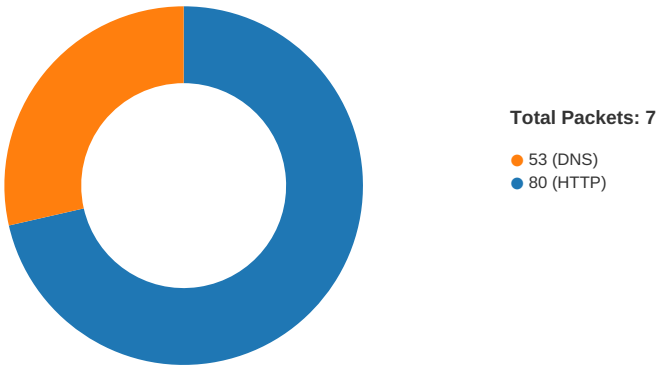
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5188.114.97.34 9798802031449 05/27/22-19:11:52.547625	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49798	80	192.168.2.5	188.114.97.3
192.168.2.5188.114.97.34 9798802031412 05/27/22-19:11:52.547625	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49798	80	192.168.2.5	188.114.97.3
192.168.2.5188.114.97.34 9798802031453 05/27/22-19:11:52.547625	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49798	80	192.168.2.5	188.114.97.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:11:52.529947996 CEST	49798	80	192.168.2.5	188.114.97.3
May 27, 2022 19:11:52.547362089 CEST	80	49798	188.114.97.3	192.168.2.5
May 27, 2022 19:11:52.547494888 CEST	49798	80	192.168.2.5	188.114.97.3
May 27, 2022 19:11:52.547625065 CEST	49798	80	192.168.2.5	188.114.97.3
May 27, 2022 19:11:52.566088915 CEST	80	49798	188.114.97.3	192.168.2.5
May 27, 2022 19:11:52.577018023 CEST	80	49798	188.114.97.3	192.168.2.5
May 27, 2022 19:11:52.577064037 CEST	80	49798	188.114.97.3	192.168.2.5
May 27, 2022 19:11:52.577187061 CEST	49798	80	192.168.2.5	188.114.97.3
May 27, 2022 19:11:52.577263117 CEST	49798	80	192.168.2.5	188.114.97.3
May 27, 2022 19:11:52.594438076 CEST	80	49798	188.114.97.3	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:11:52.497391939 CEST	61478	53	192.168.2.5	8.8.8.8
May 27, 2022 19:11:52.524352074 CEST	53	61478	8.8.8.8	192.168.2.5
May 27, 2022 19:12:35.091423035 CEST	55316	53	192.168.2.5	8.8.8.8
May 27, 2022 19:12:35.204619884 CEST	53	55316	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 19:11:52.497391939 CEST	192.168.2.5	8.8.8.8	0xd852	Standard query (0)	www.savingshk.com	A (IP address)	IN (0x0001)
May 27, 2022 19:12:35.091423035 CEST	192.168.2.5	8.8.8.8	0x3643	Standard query (0)	www.viatempo.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 19:11:52.524352074 CEST	8.8.8.8	192.168.2.5	0xd852	No error (0)	www.savingshk.com		188.114.97.3	A (IP address)	IN (0x0001)
May 27, 2022 19:11:52.524352074 CEST	8.8.8.8	192.168.2.5	0xd852	No error (0)	www.savingshk.com		188.114.96.3	A (IP address)	IN (0x0001)
May 27, 2022 19:12:35.204619884 CEST	8.8.8.8	192.168.2.5	0x3643	No error (0)	www.viatempo.com		216.120.146.201	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.savingshk.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49798	188.114.97.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:11:52.547625065 CEST	7559	OUT	GET /a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3Sf9IrYXmxrDB/U5IQUf HTTP/1.1 Host: www.savingshk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:11:52.577018023 CEST	7560	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:11:52 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 27 May 2022 18:11:52 GMT Location: https://www.savingshk.com/a5vu/?l2MHK=FVYX5&4hOD6=FXMAgLN/IrBd2h0A7KmJ0dUV04fd60Tmz3QO5NzukmZcmTlm3Sf9IrYXmxrDB/U5IQUf Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=2fygWVtW%2FKjyGrU7NWl%2BbohYlg4UfYoikT%2FUPdJB%2BdFmXDUSmP8o6%2FpJCFBE%2FfxFhcnIgb4SaX8R9Vw2Fzk%2Fmd1nna9Kad4mly7uwHyZgRnCfzu9LAusoUrkUmH4KJlKWYR0Kg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 71205f497c8d918e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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

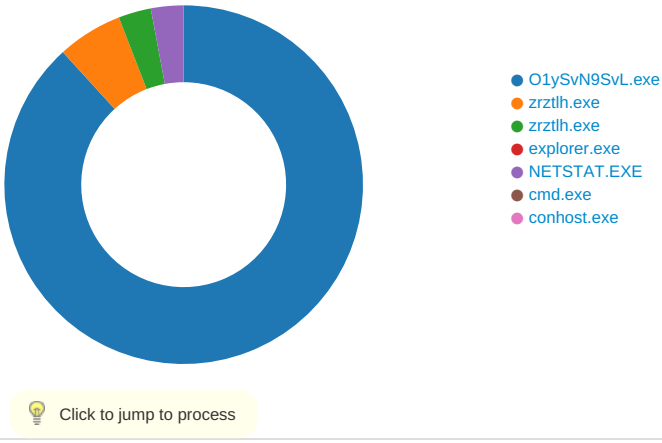
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEE
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEE

Statistics

Behavior



System Behavior

Analysis Process: O1ySvN9SvL.exe PID: 6268, Parent PID: 5876

General

Target ID:	0
Start time:	19:10:15
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\O1ySvN9SvL.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\O1ySvN9SvL.exe"
Imagebase:	0x400000
File size:	299086 bytes
MD5 hash:	CAA4C5D863A9324FA6B3A735ED446897
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: zrztlh.exe PID: 5816, Parent PID: 6268

General

Target ID:	1
Start time:	19:10:17
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\zrztlh.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\zrztlh.exe C:\Users\user\AppData\Local\Temp\kplemx
Imagebase:	0xea0000
File size:	191488 bytes
MD5 hash:	917BF3E1E68704B188F2192850C76FA6
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: 00000001.00000002.447718606.0000000000730000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.447718606.0000000000730000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.447718606.0000000000730000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 50%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kplemx	unknown	4096	success or wait	1	EAFABC	ReadFile
C:\Users\user\AppData\Local\Temp\kplemx	unknown	4096	success or wait	1	EAFABC	ReadFile

Analysis Process: zrztlh.exe PID: 6000, Parent PID: 5816

General

Target ID:	2
Start time:	19:10:17
Start date:	27/05/2022

Path:	C:\Users\user\AppData\Local\Temp\zrztlh.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\zrztlh.exe C:\Users\user\AppData\Local\Temp\kplemx
Imagebase:	0xea0000
File size:	191488 bytes
MD5 hash:	917BF3E1E68704B188F2192850C76FA6
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: 00000002.00000002.532479062.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.532479062.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.532479062.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.533348401.0000000001550000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.533348401.0000000001550000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.533348401.0000000001550000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.532198194.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.532198194.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.532198194.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.445889127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.445889127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.445889127.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.443445716.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.443445716.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.443445716.0000000000400000.00000040.00000400.00020000.00000000.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	41A427	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **6000**

General

Target ID:	3
Start time:	19:10:25
Start date:	27/05/2022
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: 00000003.00000000.509506176.0000000005327000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.509506176.0000000005327000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.509506176.0000000005327000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.489068141.0000000005327000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.489068141.0000000005327000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.489068141.0000000005327000.00000040.00000001.00040000.00000000.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: NETSTAT.EXE PID: **6124**, Parent PID: **684**

General

Target ID:	10
Start time:	19:10:59
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x1180000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.716381096.0000000000E70000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.716275585.0000000000E30000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.716275585.0000000000E30000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.716275585.0000000000E30000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.715399968.00000000007C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.715399968.00000000007C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.715399968.00000000007C0000.00000040.80000000.00040000.00000000.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	7DA427	NtReadFile

Analysis Process: cmd.exe PID: **6396**, Parent PID: **6124**

General

Target ID:	12

Start time:	19:11:03
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\zrztlh.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: **5704**, Parent PID: **6396**

General

Target ID:	13
Start time:	19:11:05
Start date:	27/05/2022
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