




**ID:** 433173
**Sample Name:** 2435.bat
**Cookbook:** default.jbs
**Time:** 12:11:53
**Date:** 11/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents


Table of Contents 2
Analysis Report 2435.bat 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 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: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
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 12
Public 12
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Rich Headers 20
Data Directories 20
Sections 20
Resources 20
Imports 20
Possible Origin 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 21
TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 21
HTTP Packets 21
Code Manipulations 23


Copyright Joe Security LLC 2021

User Modules 23
Hook Summary 23
Processes 23
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: 2435.exe PID: 6304 Parent PID: 5732 23
General 23
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Analysis Process: 2435.exe PID: 6340 Parent PID: 6304 24
General 24
File Activities 25
File Read 25
Analysis Process: explorer.exe PID: 3472 Parent PID: 6340 25
General 25
File Activities 25
Analysis Process: control.exe PID: 6932 Parent PID: 3472 25
General 25
File Activities 26
File Read 26
Analysis Process: cmd.exe PID: 3584 Parent PID: 6932 26
General 26
File Activities 26
Analysis Process: conhost.exe PID: 6292 Parent PID: 3584 26
General 26
Disassembly 27
Code Analysis 27

Copyright Joe Security LLC 2021

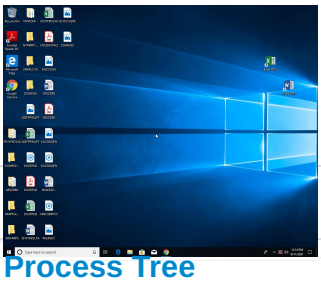
# Analysis Report 2435.bat

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 2435.bat (renamed file extension from bat to exe) |
| Analysis ID: | 433173 |
| MD5: | 862b4c2abad2c0.. |
| SHA1: | c78f0a59312c790.. |
| SHA256: | c347c2d7579053.. |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

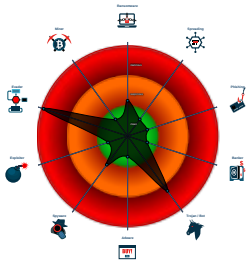
FormBook

| | |
|---|---|
| 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…
- Snort IDS alert for network traffic (e….
- 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…

### Classification



## Process Tree

- **System is w10x64**
- 2435.exe (PID: 6304 cmdline: 'C:\Users\user\Desktop\2435.exe' MD5: 862B4C2ABAD2C07AC13D5E051C18AB86)
  - 2435.exe (PID: 6340 cmdline: 'C:\Users\user\Desktop\2435.exe' MD5: 862B4C2ABAD2C07AC13D5E051C18AB86)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6932 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 3584 cmdline: /c del 'C:\Users\user\Desktop\2435.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6292 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 |
|---|---|---|---|---|
| 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

Copyright Joe Security LLC 2021

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x18409:$sqlite3step: 68 34 1C 7B E1<br>• 0x1851c:$sqlite3step: 68 34 1C 7B E1<br>• 0x18438:$sqlite3text: 68 38 2A 90 C5<br>• 0x1855d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1844b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x18573:$sqlite3blob: 68 53 D8 7F 8C |
| 00000001.00000002.288063983.0000000000590000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000001.00000002.288063983.0000000000590000.00000040.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c32a:$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 |
|---|---|---|---|---|
| 0.2.2435.exe.24d0000.3.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 0.2.2435.exe.24d0000.3.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 0.2.2435.exe.24d0000.3.raw.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x18409:$sqlite3step: 68 34 1C 7B E1<br>• 0x1851c:$sqlite3step: 68 34 1C 7B E1<br>• 0x18438:$sqlite3text: 68 38 2A 90 C5<br>• 0x1855d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1844b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x18573:$sqlite3blob: 68 53 D8 7F 8C |
| 1.2.2435.exe.400000.0.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 1.2.2435.exe.400000.0.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 13 entries | | | | |

Copyright Joe Security LLC 2021

## Sigma Overview

No Sigma rule has matched

## Signature Overview

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:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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)

### 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:



Copyright Joe Security LLC 2021

Yara detected FormBook

**Remote Access Functionality:**

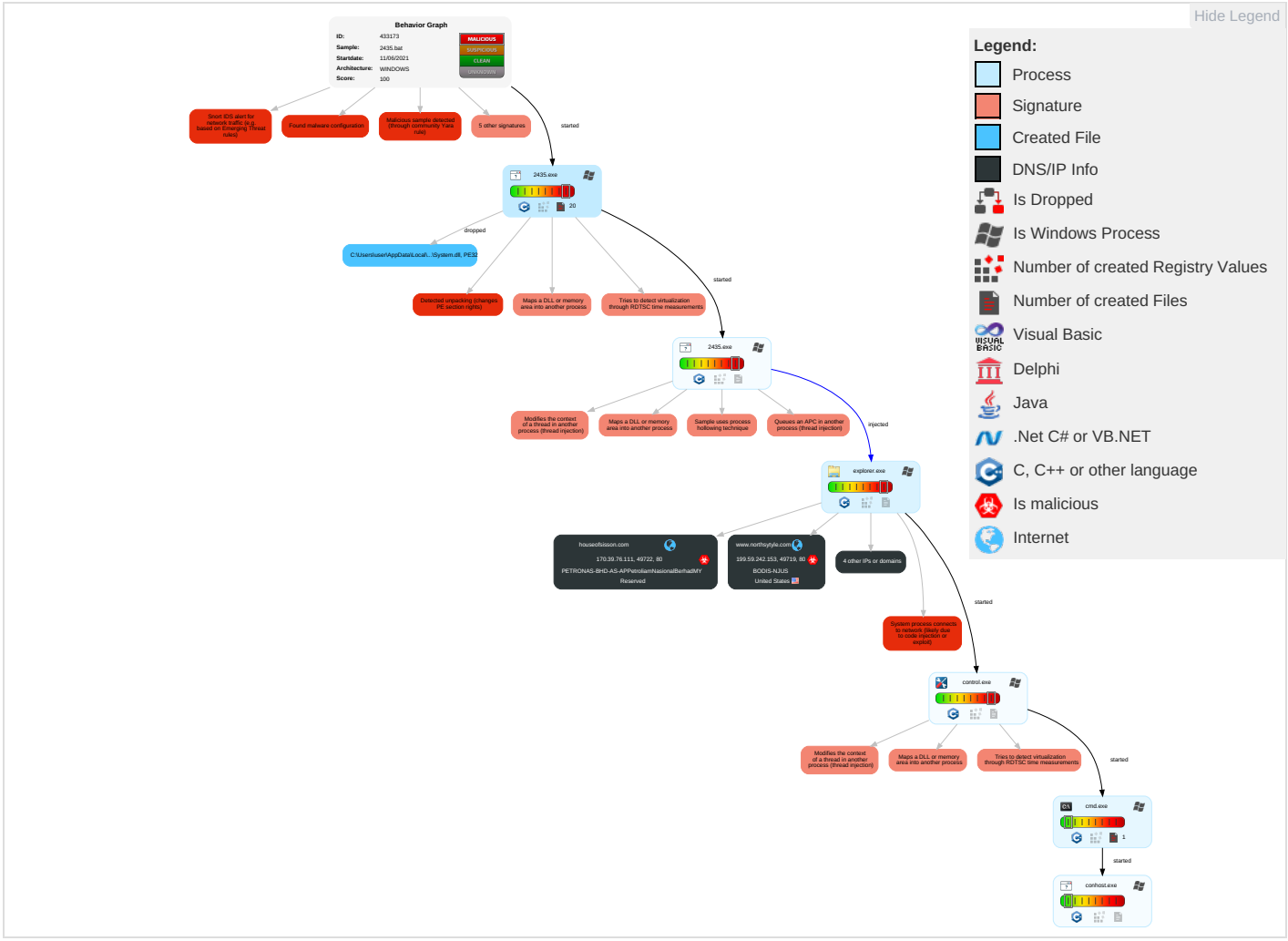


Yara detected FormBook

## 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 | Native API 1 | Path Interception | Process Injection 5 1 2 | 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 | Shared Modules 1 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 3 | LSASS Memory | Virtualization/Sandbox Evasion 3 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit SS7 to Redirect Phor Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 5 1 2 | Security Account Manager | Process Discovery 2 | SMB/Windows Admin Shares | Clipboard Data 1 | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 to Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Deobfuscate/Decode Files or Information 1 | NTDS | Remote System Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 2 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 2 | 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 | Software Packing 1 1 | Cached Domain Credentials | System Information Discovery 1 3 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

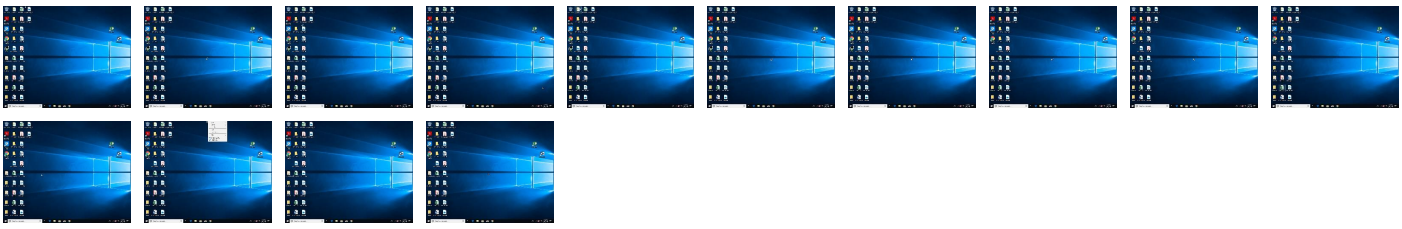
## Behavior Graph




# 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 |
|---|---|---|---|---|
| 2435.exe | 43% | ReversingLabs | Win32.Backdoor.Mokes | |
| 2435.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nsq166.tmp\System.dll | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsq166.tmp\System.dll | 0% | ReversingLabs | | |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 1.1.2435.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 1.2.2435.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 0.2.2435.exe.24d0000.3.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 9.2.control.exe.4d7f834.4.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 9.2.control.exe.43b090.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 0.0.2435.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1137482 | | Download File |
| 0.2.2435.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1137482 | | Download File |
| 1.0.2435.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1137482 | | Download File |

Copyright Joe Security LLC 2021

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.shitarpa.net/dxe/?EDHT4Ftp=ZFID08xwVlalm506aQGgsOSl52s9DuDXoXMfw5zeIfbqYw75iNwFl9ES5v0dFSHahSDk&Wj0xll=4hH838s0e | 0% | Avira URL Cloud | safe | |
| http://www.northsytyle.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W | 0% | Avira URL Cloud | 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.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.houseofsisson.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDIfcs4UgdcjH3F+Zkgn1eRT | 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.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://houseofsisson.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDI | 0% | Avira URL Cloud | 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 | |
| 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 |
|---|---|---|---|---|---|
| www.northsytyle.com | 199.59.242.153 | true | true | | unknown |
| houseofsisson.com | 170.39.76.111 | true | true | | unknown |
| shitarpa.net | 34.102.136.180 | true | false | | unknown |
| www.shitarpa.net | unknown | unknown | true | | unknown |
| www.houseofsisson.com | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.shitarpa.net/dxe/?EDHT4Ftp=ZFID08xwVlalm506aQGgsOSl52s9DuDXoXMfw5zeIfbqYw75iNwFl9ES5v0dFSHahSDk&Wj0xll=4hH838s0e | false | • Avira URL Cloud: safe | unknown |
| http://www.northsytyle.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W | true | • Avira URL Cloud: safe | unknown |
| http://www.houseofsisson.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDIfcs4Ugdcj4ECH3F+Zkgn1eRT | true | • Avira URL Cloud: safe | unknown |
| www.knighttechinca.com/dxe/ | true | • Avira URL Cloud: safe | low |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 199.59.242.153 | www.northsytyle.com | United States | | 395082 | BODIS-NJUS | true |
| 34.102.136.180 | shitarpa.net | United States | | 15169 | GOOGLEUS | false |
| 170.39.76.111 | houseofsisson.com | Reserved | | 139776 | PETRONAS-BHD-AS-APPetroliamNasionalBerhad MY | true |

### Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 433173 |
| Start date: | 11.06.2021 |
| Start time: | 12:11:53 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 17s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 2435.bat (renamed file extension from bat 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: | 29 |

| | |
|---|---|
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@7/4@3/4 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 23.8% (good quality ratio 22%)<br>• Quality average: 76.3%<br>• Quality standard deviation: 29.9% |
| HCA Information: | • Successful, ratio: 89%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 199.59.242.153 | ] New Order Vung Ang TPP Viet Nam.exe | Get hash | malicious | Browse | • www.greenshirecommons.com/un8c/?8p=mBlnh5cldNPXtcmrZbSjCDRuhUw9cugXgXVTMTkNCQGRZTLNWcZvUlnJwuwR4xQFHfof&h6Z=FZOTUTGPt4- |
| | fD56g4DRzG.exe | Get hash | malicious | Browse | • www.frontpagesweb.net/w88t/?1bWl=DwAbJomwIIUam/8Lxif0xJyCLP0/MlDCQn/X6EWMKnqqCjXzJeuBHxh9ROI30kSy7fCE&z6z=STRxNL2x |
| | malware300.docm | Get hash | malicious | Browse | • ww25.gokeenakte.top/admin.php?f=1&subid1=20210605-2000-3553-b2c5-4eab817b0105 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Payment.exe | Get hash | malicious | Browse | • www.digitalgamerentals.com/ngvm/?3fl00=eXBfF5JabAMvoJeV+Y5ra8EK8SdWvzGjXwXzLVFQuPc9hZ/16jkYHGAZEYy2Tm7CaklT&9rdLfJ=i48HtpdXmp |
| | PROFORMA INVOICE PDF.exe | Get hash | malicious | Browse | • www.chrispricellc.com/owws/?y8z=/Zb3FoJdV7HG6COtxpXcx+uQ7VrNir73csK26ufEZgOwDpn6qCuxbbRH6zNTHuB4YMFv&UDKPKv=04i8JpzhsHVX |
| | Order.exe | Get hash | malicious | Browse | • www.sweeneysservicecenter.com/jogt/?w6ATB0=U2LhZ94w5IDC+2DErQbRlpD/OzsCIaT6lUf8FwZRqb7l7kFTMUkxaoKrt4WuZdpJEkCM&Jxox=Er6tXhMxl |
| | INQ-741-020621-PDF.exe | Get hash | malicious | Browse | • www.hairgrowinggenius.com/pb93/?a0GLMhc=KPEvW4YRciSJiJFFNYizsATDgsgPxpmwnLISCA8VBLwfqs8m2gzQMN5Q9cE7knzB0ifR&rTqL5=0DKH1VwxRB |
| | CONTAINER DEPOSIT.exe | Get hash | malicious | Browse | • www.northsytyle.com/dxe/?nPRT_Pn=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W&k6Ad3=_vc0KnhxhJu |
| | Swift copy_9808.exe | Get hash | malicious | Browse | • www.scientiagenus.com/p6nu/?C2JdTP=eE7I+Sv8iOFRLyMlwLdgwXijBECgGV3UTircOP7TdlwQdQ324Qcldvmu NHuZw5leTbqh&z6nHM=ITnT9Fg |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | #U20ac9,770 pdf.exe | Get hash | malicious | Browse | • www.jobswithsecurityclearance.com/pux4/?Lv0h=3mylV7pVONTMNM6aC/niqCihOZ2+qzoqaVpusSVEetlxoEhqYhjCa0mWM/mNyWLbLdeFpUieiA==&VlKt=wBNl4pd0L |
| | Pdf Scen Invoice 17INV06003.exe | Get hash | malicious | Browse | • www.friendsed.com/s5cm/?O2=aT8vL+GQ5CKbWMYK7VfKTGSzb4SrkpvWRcVzxRDty813pzzqsjZ5NUDQNQmBAQnsw0DU&2d=YX9ti2PX |
| | ORDER LIST.pdf.exe | Get hash | malicious | Browse | • www.chrispricellc.com/owws/?t8l=/Zb3FoJdV7HG6COtxpXcx+uQ7VrNir73csK26ufEZgOwDpn6qCuxbbRH6whQbeNAVt45EvY6Zw==&YBZL=lxldV |
| | quote.pdf.exe | Get hash | malicious | Browse | • www.chrispricellc.com/owws/?rVEx8D=S0GhCH&RR=/Zb3FoJdV7HG6COtxpXcx+uQ7VrNir73csK26ufEZgOwDpn6qCuxbbRH6whpEvtDb7k+EvY9KA== |
| | hrUbr1mLqzggh0H.exe | Get hash | malicious | Browse | • www.poltgroup.com/onqm/?6l=doD+GTTuj0wR7clLLxImcVYaTf1RJOz68mAknHdMm+lQBhaMdEvcwimwgDNMMFRe7JRpz2F8Q==&2dm=3fklvpq0OPLdJVy |
| | packa.....(1).exe | Get hash | malicious | Browse | • www.educationstarcorp.com/wdva/?kfD4qZ=xabDW6gRomVRJCfQhE+1Y8vLHDgRz3GtPRqb2ZQ8ev+ZOg56Covo/3nqdMEaAH6lCy+g&kr0=dbF0vFoPNvL |
| | Pdf MT103 - Remittance.pdf.exe | Get hash | malicious | Browse | • www.ultimateplumpudding.co.uk/s5cm/?kR-4q=E2OK2mHSQGkTABA7rh5rFu9YJ97LBg918ZBY5I6VyKJbM1VF4fyc5eTvcYaTxAWeq+U4CfyJeQ==&P0D=Atxturd |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | henry.exe | Get hash | malicious | Browse | • www.booster.guru/aipc/?MZg=BMi4rIX3OaRmAVdWmHwDy158GXvJowW6rsMkLX8T/SeurUfZZjefoMGqIKxJ2f9Kzzfm&zTxX=ApdHHR |
| | Ohki Blower Skid Base Enquiry 052521.exe | Get hash | malicious | Browse | • www.greenshirecommons.com/un8c/?vR=Ltxx&5j9=mBlnh5cldNPXtcmrZbSjCDRuhUw9cugXgXVTMTkNCQGRZTLNWcZvUlnJwtQB3QA9Z6BY |
| | porosi e re Fature Proforma.exe | Get hash | malicious | Browse | • www.fux.xyz/nt8e/?v2Mp4=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&jJBP5D=-ZpPy |
| | CamScanner 24.05.2021 10.01.exe | Get hash | malicious | Browse | • www.pacificsoucre.com/ainq/?Nji0Xf=8p7tvpAP&mlvx=pIngp1ZjDfSyLzoneSC3xwzm0h2uYzOW09iGJacWdr+L3f1uJRS1s7wexdcfTOtLplEo |
| 170.39.76.111 | Proof of Payment.bat.exe | Get hash | malicious | Browse | • www.houseofsisson.com/dxe/?9rTd=b89ptlBx&F48lVPl=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDIfcs4Ugdcj4ECH0luWFwfr74U |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| www.northsytyle.com | CONTAINER DEPOSIT.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | 03003 NAVEENA.exe | Get hash | malicious | Browse | • 199.59.242.153 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| BODIS-NJUS | ] New Order Vung Ang TPP Viet Nam.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | fD56g4DRzG.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | malware300.docm | Get hash | malicious | Browse | • 199.59.242.153 |
| | Payment.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | PROFORMA INVOICE PDF.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | Order.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | INQ-741-020621-PDF.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | CONTAINER DEPOSIT.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | Swift copy_9808.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | S5.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | #U20ac9,770 pdf.exe | Get hash | malicious | Browse | • 199.59.242.153 |

Copyright Joe Security LLC 2021

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Pdf Scen Invoice 17INV06003.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | ORDER LIST.pdf.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | quote.pdf.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | hrUbr1mLqzggh0H.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | packa.....(1).exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | Pdf MT103 - Remittance.pdf.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | henry.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | Ohki Blower Skid Base Enquiry 052521.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| | porosi e re Fature Proforma.exe | Get hash | malicious | Browse | • 199.59.242.153 |
| PETRONAS-BHD-AS-APPetroliamNasionalBerhadMY | Proof of Payment.bat.exe | Get hash | malicious | Browse | • 170.39.76.111 |
| | networkservice | Get hash | malicious | Browse | • 170.38.30.47 |

## JA3 Fingerprints

**No context**

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nsq166.tmp\System.dll | INVOICE.exe | Get hash | malicious | Browse | |
| | Shipment Invoice & Consignment Notification.exe | Get hash | malicious | Browse | |
| | KY4cmAI0jU.exe | Get hash | malicious | Browse | |
| | 5t2CmTUhKc.exe | Get hash | malicious | Browse | |
| | 8qdfmqz1PN.exe | Get hash | malicious | Browse | |
| | New Order PO2193570O1.doc | Get hash | malicious | Browse | |
| | L2.xlsx | Get hash | malicious | Browse | |
| | Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx | Get hash | malicious | Browse | |
| | New Order PO2193570O1.pdf.exe | Get hash | malicious | Browse | |
| | 2320900000000.exe | Get hash | malicious | Browse | |
| | CshpH9OSkc.exe | Get hash | malicious | Browse | |
| | 5SXTKXCnqS.exe | Get hash | malicious | Browse | |
| | i6xFULh8J5.exe | Get hash | malicious | Browse | |
| | AWB00028487364 -000487449287.doc | Get hash | malicious | Browse | |
| | 090049000009000.exe | Get hash | malicious | Browse | |
| | dYy3yfSkwY.exe | Get hash | malicious | Browse | |
| | PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx | Get hash | malicious | Browse | |
| | Purchase Order Price List 061021.xlsx | Get hash | malicious | Browse | |
| | Proforma Invoice and Bank swift-REG.PI-0086547654.exe | Get hash | malicious | Browse | |
| | UGGJ4NnzFz.exe | Get hash | malicious | Browse | |

# Created / dropped Files

**C:\Users\user\AppData\Local\Temp\7us089c3e295ppclg6d9**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\2435.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 185856 |
| Entropy (8bit): | **7.99888602903792** |
| Encrypted: | **true** |
| SSDEEP: | 3072:65VNf/TDZwRRAkO7E7kbp7Vl9t2LhmgKWRqzMZa13EF9vEA5zTreL2aO+O+Ln5kB:4VNf/TDZwRWemHih7dR+h13Ev8AJTreq |
| MD5: | 1627D711EE3FADA81CB858B5682C85D2 |
| SHA1: | EFB13FDD0B52CF4E38DB413F55E32499CCEA29C7 |
| SHA-256: | 3022E519B47BD426CB96248689E855D363BA2F4EBB55F77CF5507AB2E6738EB8 |
| SHA-512: | 81D0E226A8BD6F51248B4A9E8B955B03DA877637DBBA101BE4B374F0C80EBFE226AF3D3D1F5D18E8A6429F54B9634363E4A8BF2B8D56CAA549DCC14F54AA1AC5 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Temp\7us089c3e295ppclg6d9 | |
|---|---|
| Preview: | ....X%....}.C_Z.8.....X...+.&...\|e..,..A1a..j.....h.....".=P5.*...p.....O...0+H1..E?.N....w..VM...j.Z.ss..i..m.~...../...d_.B,...v{..(b..5w.>..'.1d.D.gd...6....U.7....3Y....d...{c8.6.;.... ..?....F....n..6.x.[.N.B.....X.H..f._.;LL....sX.....R..D..w...?....oA#SWO.N.s"....b 0l.H..od..:...v.$...=.<mc...8.2SX\...]F.2.....>a...%..L..\....}....[ek.+...=l\S.H.....k.h.....3..... TK...0"Y.'..x`.j.6.{.lj..1Ve/.V....7{.....GL..8..D..OZ..%....Q.....uY..*.{..H.O.Z0&..1@G.{k+baxKr...3....>.)....IB.....1.w..1.pm.....\. ..q....FuXK..X5.fJ.o.9B...O....E.nz.]..i..... .X[k.lY.(&...m.D..9TQm$...L7..;rF$...>q.....P.....0W..L.....4.G.2..E.R./#..A....6.d.....yk.Ns.]p..5...qnK.H.*...1H.....l.....<}&.r..5..%....n..O..:.T}..q.i....;7...<....x..Z....P.L ..u&.r.o..m..s.....q6..g.G...KX9....w-.L#[.D\...O..[....V...@.1...{...LDV<W.wG.Y...^.=.(..7.W..V.<...'hh..k.t...../....MU....R.....G...../..P5.rSM 0T. |

| C:\Users\user\AppData\Local\Temp\nsq165.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\2435.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 282767 |
| Entropy (8bit): | 7.422689004181164 |
| Encrypted: | false |
| SSDEEP: | 6144:ydiVNf/TDZwRWemHih7dR+h13Ev8AJTreji+iLBB02OVaDut:1xFwE/mZRKEv8AVejqLBBFOVAm |
| MD5: | 2213022F76B392D6513DB66830C31224 |
| SHA1: | F6E1A73360DE6224A5ADB6A72486DACD7D8680C1 |
| SHA-256: | F47B6AB6DFAC7A60DEEC2078801BFF19C808BB3485E6A56A9214FE81F979A1A7 |
| SHA-512: | D1E4C16D19F210FB0E2F93BB652BA8D9F0F05985BECE148BF075A233A394B20B8FA303CDEE1CFC5B80E3A3B628F65A1B6ABF1C5B0C31525A969F04DFD67574 9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .m.....,.....LP.....8l.....m.....#..... .....J.....j.....W..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\nsq166.tmp\System.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\2435.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 11776 |
| Entropy (8bit): | 5.855045165595541 |
| Encrypted: | false |
| SSDEEP: | 192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4 |
| MD5: | FCCFF8CB7A1067E23FD2E2B63971A8E1 |
| SHA1: | 30E2A9E137C1223A78A0F7B0BF96A1C361976D91 |
| SHA-256: | 6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E |
| SHA-512: | F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C |
| Malicious: | false |
| Antivirus: | • Antivirus: Metadefender, Detection: 0%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Joe Sandbox View: | • Filename: INVOICE.exe, Detection: malicious, Browse<br>• Filename: Shipment Invoice & Consignment Notification.exe, Detection: malicious, Browse<br>• Filename: KY4cmAI0jU.exe, Detection: malicious, Browse<br>• Filename: 5t2CmTUhKc.exe, Detection: malicious, Browse<br>• Filename: 8qdfmqz1PN.exe, Detection: malicious, Browse<br>• Filename: New Order PO2193570O1.doc, Detection: malicious, Browse<br>• Filename: L2.xlsx, Detection: malicious, Browse<br>• Filename: Agency Appointment VSL Tbn-Port-Appointment Letter- 2100133.xlsx, Detection: malicious, Browse<br>• Filename: New Order PO2193570O1.pdf.exe, Detection: malicious, Browse<br>• Filename: 2320900000000.exe, Detection: malicious, Browse<br>• Filename: CshpH9OSkc.exe, Detection: malicious, Browse<br>• Filename: 5SXTKXCnqS.exe, Detection: malicious, Browse<br>• Filename: i6xFULh8J5.exe, Detection: malicious, Browse<br>• Filename: AWB00028487364 -000487449287.doc, Detection: malicious, Browse<br>• Filename: 090049000009000.exe, Detection: malicious, Browse<br>• Filename: dYy3yfSkwY.exe, Detection: malicious, Browse<br>• Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse<br>• Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse<br>• Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse<br>• Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse |
| Reputation: | moderate, very likely benign file |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\sbmborptcxfjep | |
|---|---|
| Process: | C:\Users\user\Desktop\2435.exe |
| File Type: | data |

| C:\Users\user\AppData\Local\Temp\sbmborptcxfjep | |
|---|---|
| Category: | dropped |
| Size (bytes): | 57185 |
| Entropy (8bit): | 4.984632645340986 |
| Encrypted: | false |
| SSDEEP: | 768:/7VNqmd/WNWRdN9UKYDnr3ArvJcXBFRW45fZ2SjL0djJsa7FqkcKHqTW4ipLc4+C:Hb/W4dNmr34vSXR5h2O0Dsa7k8p+UQS |
| MD5: | D3A1658292AB20E82B114799AE33644E |
| SHA1: | 71FFB4BCD29917B2E177AFA1D5B9B30056DA6FA6 |
| SHA-256: | AD00C8FCF5DCE9F7CDA163E7746E1070BDC50F0791664731F8F9AA226741E57E |
| SHA-512: | DB81E4EAC967E36DF3115A51F628492D8EC369D34202ECA31BCE6A8C0974B585F7866EBE7668AC9C5309EC3CAACEEB57023C1C3C1F72F13DA0DB7D9F1EC04F8 |
| Malicious: | false |
| Reputation: | low |
| Preview: | U... ...#.....>.....u.....e.....e.....9.....'.....a.....e.....9.....9.....\.....e.....e.....e.....u.....e.....e.....e.....e.....s. .....!.....".....#...#.$...e.%...e.&.....'.....(.....).....*.....+.....,.....-......./.....0.....1.....2.....3.....4...8.5...A.6.....7.....8...%.9.....:...e.;...e.<...e.=.....>.....?.....@...d.A...d.B...d.C.....D.....E...!.F.....G.....H...%.I...e.J.....K...s.L.....M.....N...!.O...#.P...e.Q...e.R.....S.....T...!.U.....V.....W.....X...!.Y.....Z.....[...%.\.....]....^....._...%.`...8.a...A.b.....c.....d.....e...].f...e.g...e.h...e.i.....j.....k.....l...d.m...d.n...d.o.....p.....q.....r.....s.....t.....u...e.v.....w...s.x.....y.....z.....{...#.|...e.}...e.~..... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.92290852118761 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 92.16%<br>• NSIS - Nullsoft Scriptable Install System (846627/2) 7.80%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | 2435.exe |
| File size: | 241748 |
| MD5: | 862b4c2abad2c07ac13d5e051c18ab86 |
| SHA1: | c78f0a59312c7902e445c5a31d4896907e96475c |
| SHA256: | c347c2d7579053d263f6ab6eddca7bd03691ebab93b30b5caba462caa7106beb |
| SHA512: | a4972c953b97e257c9c86528aa948b38dd4bcdef0cb2e1c5a661be864ce9d305efc499f40c8e2e9187541200df5b81c5e1c364a6a5169003357ae912596425f9 |
| SSDEEP: | 6144:Ds9e9CRE9m5SmMZ0AQV3Xtx4abWlj9Jtbs:yemUlmMKAQp9tpjPtbs |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\..... |

## File Icon



| | |
|---|---|
| Icon Hash: | b2a88c96b2ca6a72 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40323c |
| 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: | TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 UTC] |

### General

| | |
|---|---|
| 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: | 099c0646ea7282d232219f8807883be0 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x5a5a | 0x5c00 | False | 0.660453464674 | data | 6.41769823686 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x7000 | 0x1190 | 0x1200 | False | 0.4453125 | data | 5.18162709925 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x9000 | 0x1af98 | 0x400 | False | 0.55859375 | data | 4.70902740305 | 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 | 0x9e0 | 0xa00 | False | 0.45625 | data | 4.51012867721 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### 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 |
|---|---|---|---|---|---|---|---|
| 06/11/21-12:13:57.288476 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49719 | 80 | 192.168.2.5 | 199.59.242.153 |
| 06/11/21-12:13:57.288476 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49719 | 80 | 192.168.2.5 | 199.59.242.153 |
| 06/11/21-12:13:57.288476 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49719 | 80 | 192.168.2.5 | 199.59.242.153 |
| 06/11/21-12:14:18.417415 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49720 | 80 | 192.168.2.5 | 34.102.136.180 |
| 06/11/21-12:14:18.417415 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49720 | 80 | 192.168.2.5 | 34.102.136.180 |
| 06/11/21-12:14:18.417415 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49720 | 80 | 192.168.2.5 | 34.102.136.180 |
| 06/11/21-12:14:18.562024 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49720 | 34.102.136.180 | 192.168.2.5 |

Copyright Joe Security LLC 2021

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jun 11, 2021 12:13:56.956886053 CEST | 192.168.2.5 | 8.8.8.8 | 0x3c07 | Standard query (0) | www.northsytyle.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 12:14:18.308631897 CEST | 192.168.2.5 | 8.8.8.8 | 0x40ab | Standard query (0) | www.shitarpa.net | A (IP address) | IN (0x0001) |
| Jun 11, 2021 12:14:38.757014036 CEST | 192.168.2.5 | 8.8.8.8 | 0x6540 | Standard query (0) | www.houseofsisson.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jun 11, 2021 12:13:57.103427887 CEST | 8.8.8.8 | 192.168.2.5 | 0x3c07 | No error (0) | www.northsytyle.com | | 199.59.242.153 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 12:14:18.373300076 CEST | 8.8.8.8 | 192.168.2.5 | 0x40ab | No error (0) | www.shitarpa.net | shitarpa.net | | CNAME (Canonical name) | IN (0x0001) |
| Jun 11, 2021 12:14:18.373300076 CEST | 8.8.8.8 | 192.168.2.5 | 0x40ab | No error (0) | shitarpa.net | | 34.102.136.180 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 12:14:38.936023951 CEST | 8.8.8.8 | 192.168.2.5 | 0x6540 | No error (0) | www.houseofsisson.com | houseofsisson.com | | CNAME (Canonical name) | IN (0x0001) |
| Jun 11, 2021 12:14:38.936023951 CEST | 8.8.8.8 | 192.168.2.5 | 0x6540 | No error (0) | houseofsisson.com | | 170.39.76.111 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- www.northsytyle.com
- www.shitarpa.net
- www.houseofsisson.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49719 | 199.59.242.153 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 12:13:57.288475990 CEST | 5091 | OUT | GET /dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W HTTP/1.1<br>Host: www.northsytyle.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 12:13:57.415965080 CEST | 5092 | IN | HTTP/1.1 200 OK<br>Server: openresty<br>Date: Fri, 11 Jun 2021 10:13:57 GMT<br>Content-Type: text/html; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: close<br>X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_CWASVN2Fkx8Lz77aRYdiQgq6MD gGAsj0QbR5uqnRq7VXF0P0RHizFVKPsOkX86dPOS7L9FeqbRKHFNclm7c8RQ==<br>Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 43 57 41 53 56 4e 32 46 6b 78 38 4c 7a 37 37 61 52 59 64 69 51 67 71 36 4d 44 67 47 41 73 6a 30 51 62 52 35 75 71 6e 52 71 37 56 58 46 30 50 30 52 48 69 7a 46 56 4b 50 73 4f 6b 58 38 36 64 50 4f 53 37 4c 39 46 65 71 62 52 4b 48 46 4e 63 6c 6d 37 63 38 52 51 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65<br>Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_CWASVN2Fkx8Lz77aRYdiQgq6MDgGAsj0QbR5uqnRq7VXF0P0RHizFVKPsOkX86dPOS7L9FeqbRKHFN clm7c8RQ==><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name ="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what yo u are looking for."/></head>...[if IE 6 ]><body class="ie6"><![endif]-->...[if IE 7 ]><body class="ie7"><![endif]-->...[if IE 8 ]> <body class="ie8"><![endif]-->...[if IE 9 ]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,L U;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.5 | 49720 | 34.102.136.180 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 12:14:18.417414904 CEST | 5097 | OUT | GET /dxe/?EDHT4Ftp=ZFID08xwVlalm506aQGgsOSl52s9DuDXoXMfw5zeIfbqYw75iNwFl9ES5v0dFSHahSDk&Wj 0xll=4hH838s0e HTTP/1.1<br>Host: www.shitarpa.net<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jun 11, 2021 12:14:18.562024117 CEST | 5098 | IN | HTTP/1.1 403 Forbidden<br>Server: openresty<br>Date: Fri, 11 Jun 2021 10:14:18 GMT<br>Content-Type: text/html<br>Content-Length: 275<br>ETag: "60ba4131-113"<br>Via: 1.1 google<br>Connection: close<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 3c 2f 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> <h1>Access Forbidden</h1></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.5 | 49722 | 170.39.76.111 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 12:14:39.094999075 CEST | 5110 | OUT | GET /dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDIfcs4Ugdcj4ECH3F+Zkgn1eRT HTTP/1.1<br>Host: www.houseofsisson.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jun 11, 2021 12:14:39.417160988 CEST | 5114 | IN | HTTP/1.1 301 Moved Permanently<br>Connection: close<br>Content-Type: text/html; charset=UTF-8<br>Expires: Wed, 11 Jan 1984 05:00:00 GMT<br>Cache-Control: no-cache, must-revalidate, max-age=0<br>X-Redirect-By: WordPress<br>Location: http://houseofsisson.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=5uRqQMqQLkS85WfNP4LQlejd47xl1HHY1ecJzVPNghDIfcs4Ugdcj4ECH3F+Zkgn1eRT<br>Content-Length: 0<br>Date: Fri, 11 Jun 2021 10:14:39 GMT<br>Server: LiteSpeed |

# 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

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: 2435.exe PID: 6304 Parent PID: 5732

### General

| | |
|---|---|
| Start time: | 12:12:43 |
| Start date: | 11/06/2021 |
| Path: | C:\Users\user\Desktop\2435.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\2435.exe' |
| Imagebase: | 0x400000 |
| File size: | 241748 bytes |
| MD5 hash: | 862B4C2ABAD2C07AC13D5E051C18AB86 |
| 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: 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.236124712.00000000024D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

## File Activities

Show Windows behavior

### File Created

### File Deleted

### File Written

### File Read

## Analysis Process: 2435.exe PID: 6340 Parent PID: 6304

### General

| | |
|---|---|
| Start time: | 12:12:44 |
| Start date: | 11/06/2021 |
| Path: | C:\Users\user\Desktop\2435.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\2435.exe' |
| Imagebase: | 0x400000 |
| File size: | 241748 bytes |
| MD5 hash: | 862B4C2ABAD2C07AC13D5E051C18AB86 |
| 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: 00000001.00000002.288063983.0000000000590000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.288063983.0000000000590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.288063983.0000000000590000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.287887430.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.287887430.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.287887430.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.288110425.00000000005C0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.288110425.00000000005C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.288110425.00000000005C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.232707868.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.232707868.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.232707868.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |

| | |
|---|---|
| Reputation: | low |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: explorer.exe PID: 3472 Parent PID: 6340

### General

| | |
|---|---|
| Start time: | 12:12:49 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\explorer.exe |
| Wow64 process (32bit): | false |
| Commandline: | |
| Imagebase: | 0x7ff693d90000 |
| 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: 00000002.00000000.279389714.000000000705E000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.279389714.000000000705E000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.279389714.000000000705E000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: control.exe PID: 6932 Parent PID: 3472

### General

| | |
|---|---|
| Start time: | 12:13:09 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\SysWOW64\control.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\control.exe |
| Imagebase: | 0x340000 |
| File size: | 114688 bytes |
| MD5 hash: | 40FBA3FBFD5E33E0DE1BA45472FDA66F |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.496354910.0000000000A80000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.496354910.0000000000A80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.496354910.0000000000A80000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.497155166.0000000002FB0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.497155166.0000000002FB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.497155166.0000000002FB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | moderate |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: cmd.exe PID: 3584 Parent PID: 6932

### General

| | |
|---|---|
| Start time: | 12:13:14 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Users\user\Desktop\2435.exe' |
| Imagebase: | 0xeb0000 |
| 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** Show Windows behavior

## Analysis Process: conhost.exe PID: 6292 Parent PID: 3584

### General

| | |
|---|---|
| Start time: | 12:13:15 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7ecfc0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

Copyright Joe Security LLC 2021

# Disassembly

## Code Analysis

Copyright Joe Security LLC


Copyright Joe Security LLC 2021