
**ID:** 435312
**Sample Name:** Updated Order COA.doc
**Cookbook:** defaultwindowsofficecookbook.jbs
**Time:** 12:00:52
**Date:** 16/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

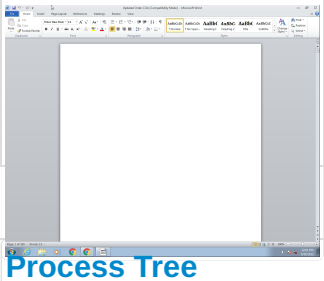
# Windows Analysis Report Updated Order COA.doc

## Overview

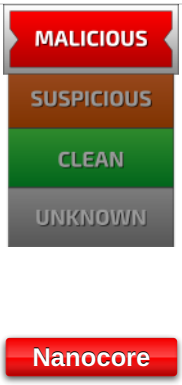
### General Information

| | |
|---|---|
| Sample Name: | Updated Order COA.doc |
| Analysis ID: | 435312 |
| MD5: | 59f9c2a162cf48f… |
| SHA1: | f8702f19bae3a9f… |
| SHA256: | 23a865d4a1205b.. |
| Tags: | doc |
| Infos: | |

Most interesting Screenshot:



### Detection

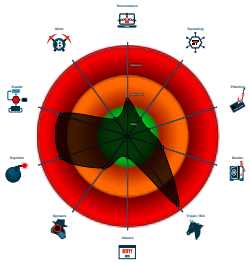



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Allocates memory in foreign process…

### Classification



## Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1748 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2624 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 098765.exe (PID: 2428 cmdline: C:\Users\Public\098765.exe MD5: 5688C69C4379841EEE42DCAEC2DBF55A)
    - RegAsm.exe (PID: 2896 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
      - schtasks.exe (PID: 2456 cmdline: 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp7790.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2536 cmdline: taskeng.exe {6204476F-CB6D-41BF-A018-07A92169AAA2} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - RegAsm.exe (PID: 2592 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe 0 MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "18773cd6-e296-4327-b004-0088e2e8",
  "Group": "WEALTH",
  "Domain1": "185.140.53.154",
  "Domain2": "wealthybillionaire.ddns.net",
  "Port": 5540,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.2359788064.00000000039 39000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000005.00000002.2359788064.00000000039 39000.00000004.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0x3185:$a: NanoCore<br>• 0x31de:$a: NanoCore<br>• 0x321b:$a: NanoCore<br>• 0x3294:$a: NanoCore<br>• 0x1693f:$a: NanoCore<br>• 0x16954:$a: NanoCore<br>• 0x16989:$a: NanoCore<br>• 0x2f933:$a: NanoCore<br>• 0x2f948:$a: NanoCore<br>• 0x2f97d:$a: NanoCore<br>• 0x31e7:$b: ClientPlugin<br>• 0x3224:$b: ClientPlugin<br>• 0x3b22:$b: ClientPlugin<br>• 0x3b2f:$b: ClientPlugin<br>• 0x166fb:$b: ClientPlugin<br>• 0x16716:$b: ClientPlugin<br>• 0x16746:$b: ClientPlugin<br>• 0x1695d:$b: ClientPlugin<br>• 0x16992:$b: ClientPlugin<br>• 0x2f6ef:$b: ClientPlugin<br>• 0x2f70a:$b: ClientPlugin |
| 00000005.00000002.2356733340.00000000009 20000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xf7ad:$x1: NanoCore.ClientPluginHost<br>• 0xf7da:$x2: IClientNetworkHost |
| 00000005.00000002.2356733340.00000000009 20000.00000004.00000001.sdmp | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xf7ad:$x2: NanoCore.ClientPluginHost<br>• 0x10888:$s4: PipeCreated<br>• 0xf7c7:$s5: IClientLoggingHost |
| 00000005.00000002.2356733340.00000000009 20000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| Click to see the 21 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 4.2.098765.exe.35098d0.9.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe38d:$x1: NanoCore.ClientPluginHost<br>• 0xe3ca:$x2: IClientNetworkHost<br>• 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 4.2.098765.exe.35098d0.9.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe105:$x1: NanoCore Client.exe<br>• 0xe38d:$x2: NanoCore.ClientPluginHost<br>• 0xf9c6:$s1: PluginCommand<br>• 0xf9ba:$s2: FileCommand<br>• 0x1086b:$s3: PipeExists<br>• 0x16622:$s4: PipeCreated<br>• 0xe3b7:$s5: IClientLoggingHost |
| 4.2.098765.exe.35098d0.9.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 4.2.098765.exe.35098d0.9.unpack | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xe0f5:$a: NanoCore<br>• 0xe105:$a: NanoCore<br>• 0xe339:$a: NanoCore<br>• 0xe34d:$a: NanoCore<br>• 0xe38d:$a: NanoCore<br>• 0xe154:$b: ClientPlugin<br>• 0xe356:$b: ClientPlugin<br>• 0xe396:$b: ClientPlugin<br>• 0xe27b:$c: ProjectData<br>• 0xec82:$d: DESCrypto<br>• 0x1664e:$e: KeepAlive<br>• 0x1463c:$g: LogClientMessage<br>• 0x10837:$i: get_Connected<br>• 0xefb8:$j: #=q<br>• 0xefe8:$j: #=q<br>• 0xf004:$j: #=q<br>• 0xf034:$j: #=q<br>• 0xf050:$j: #=q<br>• 0xf06c:$j: #=q<br>• 0xf09c:$j: #=q<br>• 0xf0b8:$j: #=q |
| 4.2.098765.exe.35098d0.9.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x1018d:$x1: NanoCore.ClientPluginHost<br>• 0x101ca:$x2: IClientNetworkHost<br>• 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 64 entries | | | | |

# Sigma Overview

## AV Detection:

**Sigma detected: NanoCore**

## Exploits:

**Sigma detected: File Dropped By EQNEDT32EXE**

## E-Banking Fraud:

**Sigma detected: NanoCore**

## System Summary:

**Sigma detected: Droppers Exploiting CVE-2017-11882**

**Sigma detected: Execution from Suspicious Folder**

**Sigma detected: Suspicious Process Start Without DLL**

**Sigma detected: Possible Applocker Bypass**

## Stealing of Sensitive Information:

**Sigma detected: NanoCore**

## Remote Access Functionality:

**Sigma detected: NanoCore**

# Signature Overview

Click to jump to signature section

## AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file

## Exploits:

- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

## Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

## E-Banking Fraud:

- Yara detected Nanocore RAT

## System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations
- Office equation editor drops PE file

## Data Obfuscation:

- .NET source code contains potential unpacker

## Boot Survival:

- Drops PE files to the user root directory
- Uses schtasks.exe or at.exe to add and modify task schedules

## Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

## HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

## Stealing of Sensitive Information:

Yara detected Nanocore RAT

## Remote Access Functionality:

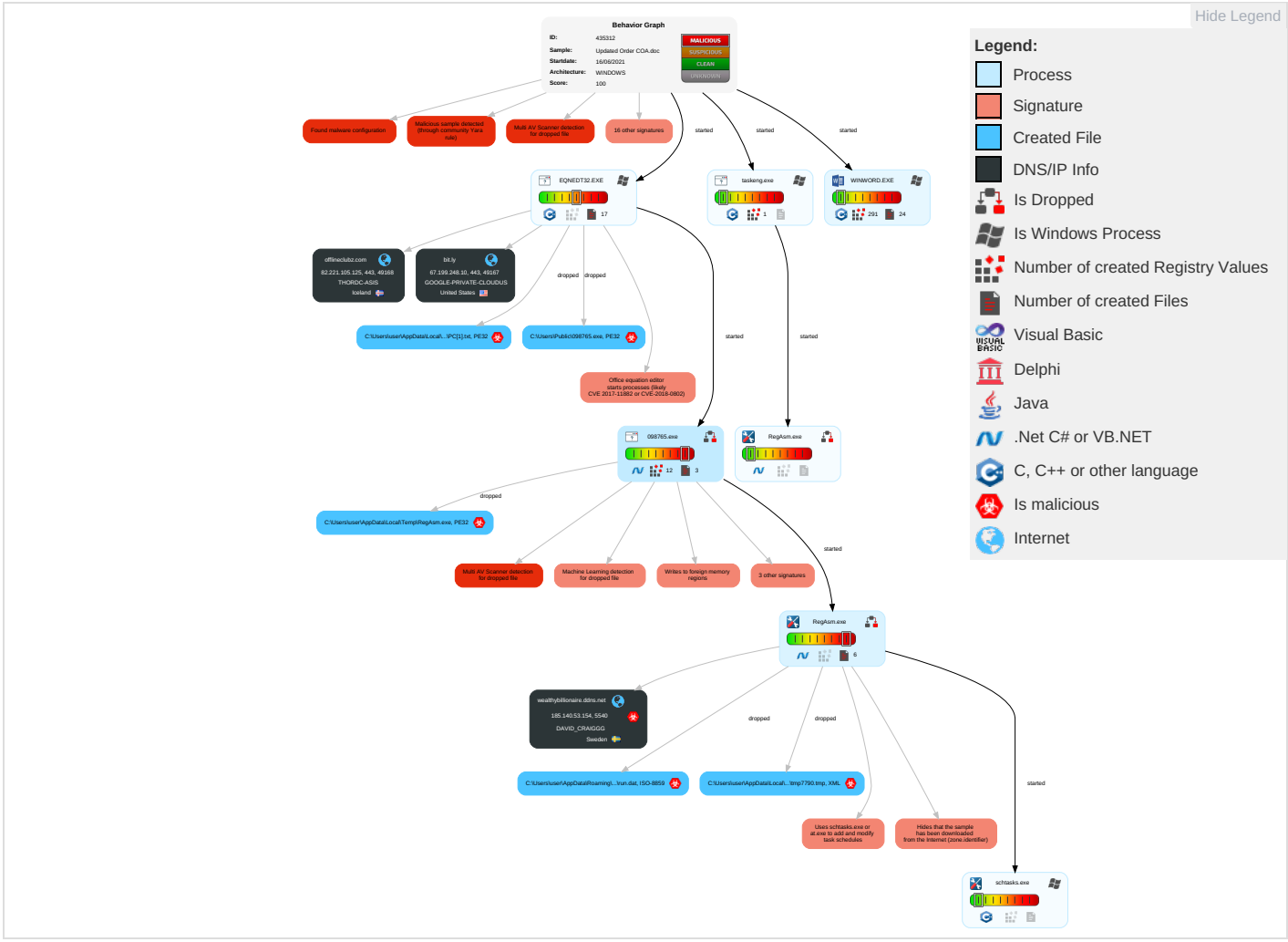
Detected Nanocore Rat

Yara detected Nanocore RAT

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Co and |
|---|---|---|---|---|---|---|---|---|---|---|
| Spearphishing Link 1 | Exploitation for Client Execution 1 3 | Valid Accounts 1 | Valid Accounts 1 | Disable or Modify Tools 1 1 | Input Capture 1 1 | File and Directory Discovery 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Ing Tra |
| Valid Accounts 1 | Command and Scripting Interpreter 1 | Scheduled Task/Job 1 | Access Token Manipulation 1 | Deobfuscate/Decode Files or Information 1 | LSASS Memory | System Information Discovery 1 3 | Remote Desktop Protocol | Input Capture 1 1 | Exfiltration Over Bluetooth | Enc Cha |
| Domain Accounts | Scheduled Task/Job 1 | Logon Script (Windows) | Process Injection 3 1 2 | Obfuscated Files or Information 2 | Security Account Manager | Security Software Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non Por |
| Local Accounts | At (Windows) | Logon Script (Mac) | Scheduled Task/Job 1 | Software Packing 1 1 | NTDS | Query Registry 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Rer Acc Sof |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Masquerading 1 2 1 | LSA Secrets | Process Discovery 2 | SSH | Keylogging | Data Transfer Size Limits | Non App Lay Pro |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Valid Accounts 1 | Cached Domain Credentials | Virtualization/Sandbox Evasion 2 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | App Lay Pro |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Access Token Manipulation 1 | DCSync | Application Window Discovery 1 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Cor Use |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Virtualization/Sandbox Evasion 2 1 | Proc Filesystem | Remote System Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | App Lay |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Process Injection 3 1 2 | /etc/passwd and /etc/shadow | System Network Connections Discovery | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | We Pro |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Hidden Files and Directories 1 | Network Sniffing | Process Discovery | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File Pro |

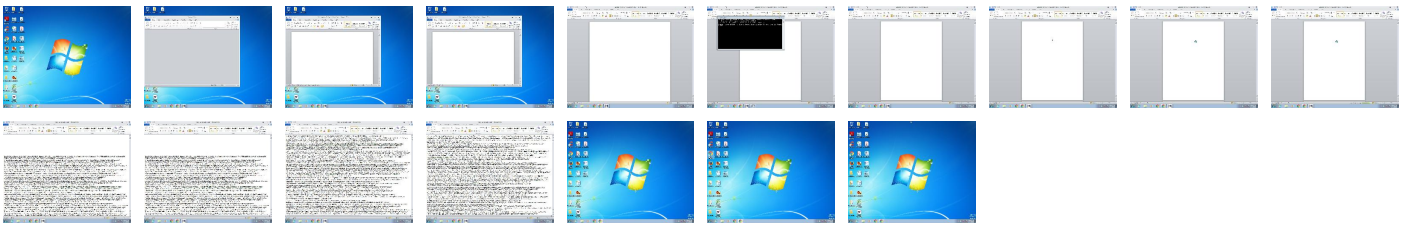
## Behavior Graph

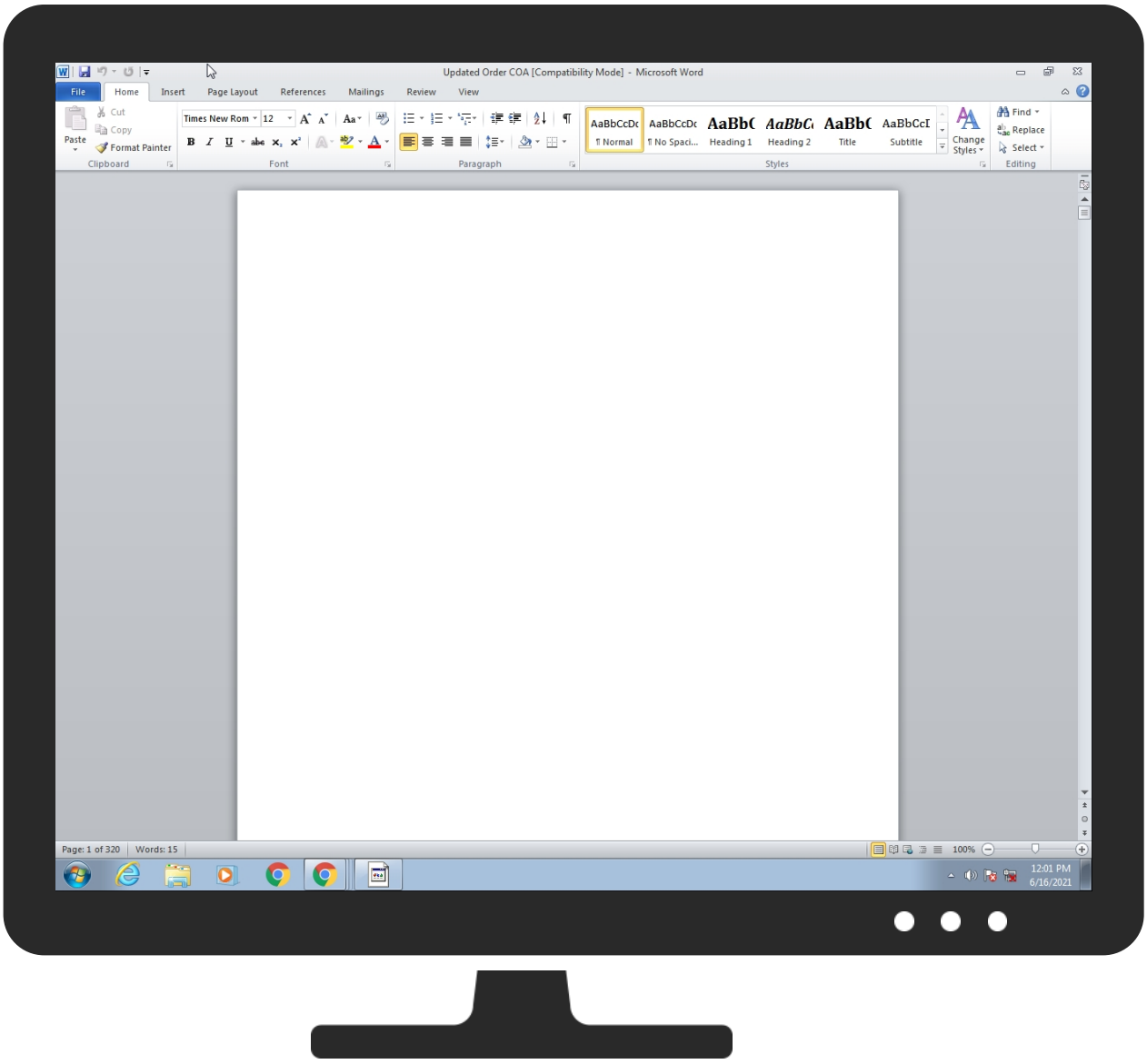



## Screenshots

### 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 |
|---|---|---|---|---|
| Updated Order COA.doc | 17% | ReversingLabs | Document-Office.Exploit.CVE-2018-0802 | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PC[1].txt | 100% | Joe Sandbox ML | | |
| C:\Users\Public\098765.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PC[1].txt | 22% | ReversingLabs | ByteCode-MSIL.Trojan.NanoBot | |
| C:\Users\user\AppData\Local\Temp\RegAsm.exe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\RegAsm.exe | 0% | ReversingLabs | | |
| C:\Users\Public\098765.exe | 22% | ReversingLabs | ByteCode-MSIL.Trojan.NanoBot | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 5.2.RegAsm.exe.920000.6.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 5.2.RegAsm.exe.400000.1.unpack | 100% | Avira | TR/Dropper.Gen | | Download File |

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ns.adobe.c/s | 0% | Avira URL Cloud | safe | |
| http://crl.pkioverheid.nl/DomOvLatestCRL.crl0 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOvLatestCRL.crl0 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOvLatestCRL.crl0 | 0% | URL Reputation | safe | |
| http://ns.ao | 0% | Avira URL Cloud | safe | |
| http://ocsp.entrust.net03 | 0% | URL Reputation | safe | |
| http://ocsp.entrust.net03 | 0% | URL Reputation | safe | |
| http://ocsp.entrust.net03 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0 | 0% | URL Reputation | safe | |
| http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0 | 0% | URL Reputation | safe | |
| http://go.microsoft. | 0% | URL Reputation | safe | |
| http://go.microsoft. | 0% | URL Reputation | safe | |
| http://go.microsoft. | 0% | URL Reputation | safe | |
| http://www.%s.comPA | 0% | URL Reputation | safe | |
| http://www.%s.comPA | 0% | URL Reputation | safe | |
| http://www.%s.comPA | 0% | URL Reputation | safe | |
| http://www.diginotar.nl/cps/pkioverheid0 | 0% | URL Reputation | safe | |
| http://www.diginotar.nl/cps/pkioverheid0 | 0% | URL Reputation | safe | |
| http://www.diginotar.nl/cps/pkioverheid0 | 0% | URL Reputation | safe | |
| http://n.f | 0% | Avira URL Cloud | safe | |
| http://ocsp.entrust.net0D | 0% | URL Reputation | safe | |
| http://ocsp.entrust.net0D | 0% | URL Reputation | safe | |
| http://ocsp.entrust.net0D | 0% | URL Reputation | safe | |
| 185.140.53.154 | 0% | Avira URL Cloud | safe | |
| wealthybillionaire.ddns.net | 0% | Avira URL Cloud | safe | |
| http://https://offlineclubz.com/PC.txt | 0% | Avira URL Cloud | safe | |
| http://ns.adobede | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| bit.ly | 67.199.248.10 | true | false | | high |
| offlineclubz.com | 82.221.105.125 | true | false | | unknown |
| wealthybillionaire.ddns.net | 185.140.53.154 | true | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| 185.140.53.154 | true | • Avira URL Cloud: safe | unknown |
| wealthybillionaire.ddns.net | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 82.221.105.125 | offlineclubz.com | Iceland | | 50613 | THORDC-ASIS | false |
| 185.140.53.154 | wealthybillionaire.ddns.net | Sweden | | 209623 | DAVID_CRAIGGG | true |
| 67.199.248.10 | bit.ly | United States | | 396982 | GOOGLE-PRIVATE-CLOUDUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 435312 |
| Start date: | 16.06.2021 |
| Start time: | 12:00:52 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 38s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Updated Order COA.doc |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2) |
| Number of analysed new started processes analysed: | 11 |
| 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.expl.evad.winDOC@11/22@9/3 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 5.5% (good quality ratio 2.6%)<br>• Quality average: 24.4%<br>• Quality standard deviation: 30.5% |
| HCA Information: | • Successful, ratio: 98%<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: .doc<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 12:01:36 | API Interceptor | 63x Sleep call for process: EQNEDT32.EXE modified |
| 12:01:40 | API Interceptor | 133x Sleep call for process: 098765.exe modified |
| 12:01:55 | API Interceptor | 1419x Sleep call for process: RegAsm.exe modified |
| 12:01:57 | API Interceptor | 2x Sleep call for process: schtasks.exe modified |
| 12:01:58 | Task Scheduler | Run new task: SMTP Service path: "C:\Users\user\AppData\Local\Temp\RegAsm.exe" s>$(Arg0) |
| 12:01:58 | API Interceptor | 357x Sleep call for process: taskeng.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 82.221.105.125 | gbqFfT54L.rtf | Get hash | malicious | Browse | • mysit.space/123//v/bGo2799 |
| | 65001078.DOC | Get hash | malicious | Browse | • uploadtops.is/1//q/grFRBQT |
| | Product list - Quotation sheet.doc | Get hash | malicious | Browse | • uploadtops.is/1//q/8oEITJq |
| | 17Revenue_doc_id4837726.exe | Get hash | malicious | Browse | • uploadtops.is/1//q/lJqqLvC |
| | Payment slip.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/NuRHVL9 |
| | 71355881.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/z132Bct |
| | ORDER_20180620.DOC | Get hash | malicious | Browse | • uploadtops.is/1//f/rihUTZ7 |
| | Product_details.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/uwkjs1U |
| | RE RE  Minimum Order Quantity 34562$$.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/RkEXBrB |
| | Provision Requisition Quotation 04.05.2018.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/PecgndH |
| | 2 Remittance Advice.doc | Get hash | malicious | Browse | • uploadtops.is/1//f/St7GsQ3 |
| | L6GuxhH6S.rtf | Get hash | malicious | Browse | • uploadtops.is/1//f/St7GsQ3 |
| 185.140.53.154 | Maersk BL & PL.exe | Get hash | malicious | Browse | |
| | Quotation.exe | Get hash | malicious | Browse | |
| | SWIFT.exe | Get hash | malicious | Browse | |
| | Qotation.exe | Get hash | malicious | Browse | |
| | SMJshb9rCD.exe | Get hash | malicious | Browse | |
| | 3z4ibRIdCl.exe | Get hash | malicious | Browse | |
| | UfQ7WpbVPG.exe | Get hash | malicious | Browse | |
| | 9ieQE1S5ZH.exe | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| bit.ly | #Ud83d#Udcde_#U25b6#Ufe0f.htm | Get hash | malicious | Browse | • 67.199.248.10 |
| | P.I-84514.doc | Get hash | malicious | Browse | • 67.199.248.11 |
| | P.I-84512.doc | Get hash | malicious | Browse | • 67.199.248.11 |
| | #Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm | Get hash | malicious | Browse | • 67.199.248.10 |
| | #Ud83d#Udcde_Message_Received_05_19_21.htm.htm | Get hash | malicious | Browse | • 67.199.248.10 |
| | #Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen.htm.htm | Get hash | malicious | Browse | • 67.199.248.10 |
| | #Ud83d#Udcde_#U25b6#Ufe0f.htm | Get hash | malicious | Browse | • 67.199.248.10 |
| | #U266b Audio_47920.wavv - - Copy.html | Get hash | malicious | Browse | • 67.199.248.11 |
| | #Ud83d#Udcde_#U25b6#Ufe0fPlay_to_Listen htm.htm | Get hash | malicious | Browse | • 67.199.248.11 |
| | kSfW7fFDWa.rtf | Get hash | malicious | Browse | • 67.199.248.10 |
| | 2020tb3005.doc__.rtf | Get hash | malicious | Browse | • 67.199.248.11 |
| | -Recibo de pago.doc | Get hash | malicious | Browse | • 67.199.248.11 |
| | Lingarogroup_Scan_item.htm | Get hash | malicious | Browse | • 67.199.248.11 |
| | itOr6lv1UH.exe | Get hash | malicious | Browse | • 67.199.248.11 |
| | Qgc2Nreer3.exe | Get hash | malicious | Browse | • 67.199.248.11 |
| | purchase inquiry 25.5.2021.doc__.rtf | Get hash | malicious | Browse | • 67.199.248.10 |
| | purchase order.doc | Get hash | malicious | Browse | • 67.199.248.11 |
| | #Ud83d#Udcde(801) 451.htm | Get hash | malicious | Browse | • 67.199.248.10 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Revise Order Sheets.doc | Get hash | malicious | Browse | • 67.199.248.11 |
| | Payoff - 2021AT0514.doc | Get hash | malicious | Browse | • 67.199.248.10 |
| wealthybillionaire.ddns.net | Revise Order Sheets.doc | Get hash | malicious | Browse | • 79.134.225.52 |
| | TT SWIFT COPY.exe | Get hash | malicious | Browse | • 41.217.65.85 |
| | bedrapes.exe | Get hash | malicious | Browse | • 154.118.68.3 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| DAVID_CRAIGGG | Payment confirmation.exe | Get hash | malicious | Browse | • 185.140.53.45 |
| | 03soKqWLfN.exe | Get hash | malicious | Browse | • 185.140.53.145 |
| | installer.exe | Get hash | malicious | Browse | • 185.140.53.145 |
| | Maersk BL & PL.exe | Get hash | malicious | Browse | • 185.140.53.154 |
| | vmw7WdkJ6k.exe | Get hash | malicious | Browse | • 185.140.53.12 |
| | ORDER.exe | Get hash | malicious | Browse | • 185.140.53.135 |
| | ORDER-21611docx.exe | Get hash | malicious | Browse | • 185.165.153.116 |
| | 6VYNUalwUt.exe | Get hash | malicious | Browse | • 185.244.30.92 |
| | ORDER-6010.pdf.exe | Get hash | malicious | Browse | • 185.244.30.92 |
| | CONTRACT.exe | Get hash | malicious | Browse | • 185.140.53.135 |
| | doc030273202105211733O5IMG0012.exe | Get hash | malicious | Browse | • 185.140.53.230 |
| | yfilQwrYpA.exe | Get hash | malicious | Browse | • 185.140.53.216 |
| | Ff6m4N8pog.exe | Get hash | malicious | Browse | • 185.140.53.216 |
| | yCdBrRiAN2.exe | Get hash | malicious | Browse | • 185.140.53.216 |
| | loKHQzx6Lf.exe | Get hash | malicious | Browse | • 185.140.53.216 |
| | SecuriteInfo.com.Program.Win32.Wacapew.Cml.7225.exe | Get hash | malicious | Browse | • 185.140.53.129 |
| | Shipping Documents_Bill of Lading 910571880.exe | Get hash | malicious | Browse | • 185.140.53.129 |
| | knqh5Hw6gu.exe | Get hash | malicious | Browse | • 185.140.53.13 |
| | Container_Deposit_slip_pdf.jar | Get hash | malicious | Browse | • 185.244.30.47 |
| | Cargo Charter Request details.vbs | Get hash | malicious | Browse | • 185.244.30.184 |
| THORDC-ASIS | i | Get hash | malicious | Browse | • 82.221.103.244 |
| | Factura_202768456912.html | Get hash | malicious | Browse | • 82.221.141.10 |
| | sMjtvTsYf5.exe | Get hash | malicious | Browse | • 192.253.250.161 |
| | yVn2ywuhEC.exe | Get hash | malicious | Browse | • 82.221.103.244 |
| | FickerStealer.exe | Get hash | malicious | Browse | • 82.221.131.102 |
| | isb777amx.exe | Get hash | malicious | Browse | • 82.221.131.5 |
| | uTorrent.exe | Get hash | malicious | Browse | • 82.221.103.245 |
| | 9ISF FILLING 10+.exe | Get hash | malicious | Browse | • 82.221.136.4 |
| | 67Final Draft ISF 10+2 Fillin.exe | Get hash | malicious | Browse | • 82.221.113.145 |
| | 47Abusive  Email Letter.exe | Get hash | malicious | Browse | • 82.221.129.19 |
| | 14INV NO.35839 - 2018.doc | Get hash | malicious | Browse | • 82.221.129.19 |
| | 7REQUEST FOR QUOTE LIST-pdf.exe | Get hash | malicious | Browse | • 82.221.129.19 |
| | 19Document-pdf.exe | Get hash | malicious | Browse | • 82.221.129.19 |
| | 11112837654201809.doc | Get hash | malicious | Browse | • 82.221.129.19 |
| | 35doc43288920180918.doc | Get hash | malicious | Browse | • 82.221.129.19 |
| | 23NF-DOC865443.doc | Get hash | malicious | Browse | • 82.221.129.19 |
| | 63Document-2.exe | Get hash | malicious | Browse | • 82.221.129.19 |
| | 18PO45433.doc | Get hash | malicious | Browse | • 82.221.129.19 |
| | 17po029222.exe | Get hash | malicious | Browse | • 82.221.129.19 |
| | 30Abusive Email Letter.exe | Get hash | malicious | Browse | • 82.221.129.19 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 7dcce5b76c8b17472d024758970a406b | tender-156639535.xlsm | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | Agenda1.docx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | tender-2038988342.xlsm | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | Citibank Payment Advice.xlsx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | sentence-1711450431.xlsm | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | RFQ Products.xlsx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | Tax Document.docx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | hG6FzLXtsf.xls | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | P0fhg2Duqa.xls | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | GENERAL DYNAMICS_WIRE_REMITTANCE.xlsx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | GENERAL DYNAMICS_WIRE_REMITTANCE_virus_scan.xlsx | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.13632.rtf | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | RFQ SI-01.08.062021.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | REQ-54265-CSE-445.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | RFQ-Excel-NPF0140621.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | RFQ#176220621.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | Purchase Order.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | Purchase Order.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | New Order PO2193570O1.doc | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |
| | document-47-2637.xls | Get hash | malicious | Browse | • 82.221.105.125<br>• 67.199.248.10 |

## Dropped Files

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\RegAsm.exe | Ref 0180066743.xlsx | Get hash | malicious | Browse | |
| | Purchase Order Price List.xlsx | Get hash | malicious | Browse | |
| | Quote QU038097.doc | Get hash | malicious | Browse | |
| | 6Cprm97UTI.xls | Get hash | malicious | Browse | |
| | Payment_Confirmation_Slip.xlsx | Get hash | malicious | Browse | |
| | Overdue Invoice.xlsx | Get hash | malicious | Browse | |
| | Quotation.xlsx | Get hash | malicious | Browse | |
| | ENCLOSE ORDER LIST.xlsx | Get hash | malicious | Browse | |
| | PO INV 195167 & 195324.xlsx | Get hash | malicious | Browse | |
| | Bank letter.xlsx | Get hash | malicious | Browse | |
| | Quotation.xlsx | Get hash | malicious | Browse | |
| | PO 19030004.xlsx | Get hash | malicious | Browse | |
| | New PO  PO20.xlsx | Get hash | malicious | Browse | |
| | ORDER LIST.xlsx | Get hash | malicious | Browse | |
| | RFQ 00112.xlsx | Get hash | malicious | Browse | |
| | inquiry.xlsx | Get hash | malicious | Browse | |

# Created / dropped Files

**C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506**

| | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | Microsoft Cabinet archive data, 60080 bytes, 1 file |
| Category: | dropped |
| Size (bytes): | 60080 |
| Entropy (8bit): | **7.995256720209506** |
| Encrypted: | **true** |
| SSDEEP: | 768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4 |
| MD5: | 6045BACCF49E1EBA0E674945311A06E6 |
| SHA1: | 379C6234849EECEDE26FAD192C2EE59E0F0221CB |
| SHA-256: | 65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58 |
| SHA-512: | DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 | |
|---|---|
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0.....<br>..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&.<br>..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..\|[.w.M.!<-<br>.}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8SI...E".h...*.....ItVs.K.....<br>.3.9.I..`D..e.i`....y....,.5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F. |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 893 |
| Entropy (8bit): | 7.366016576663508 |
| Encrypted: | false |
| SSDEEP: | 24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x |
| MD5: | D4AE187B4574036C2D76B6DF8A8C1A30 |
| SHA1: | B06F409FA14BAB33CBAF4A37811B8740B624D9E5 |
| SHA-256: | A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7 |
| SHA-512: | 1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646B<br>C |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | 0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930<br>140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~<br>..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....<br>....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.<br>X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1. |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 328 |
| Entropy (8bit): | 3.1202775039435013 |
| Encrypted: | false |
| SSDEEP: | 6:kKXx6yMEe8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:P8k8kPlE99SNxAhUe3OMx |
| MD5: | 48AAC9E7FEAD1053A0FA1B4E07DC7919 |
| SHA1: | 4356801A6D304881B661B1E7FE24B4124BB152F6 |
| SHA-256: | 14BE10736942859BA83102FA16C77C1081861A12A9E741AFE502335F8641203A |
| SHA-512: | 1E10781556327E96C61FEEDAFEEC4418191F6F7061DFF1A78950ACA0654FC711C72AB1EB759E0E51E34B151EB714AEF20D6213FFE9183A4E3D915216DA3B4FB |
| Malicious: | false |
| Reputation: | low |
| Preview: | p..... .....V.T..b..(..... .....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.<br>s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."... |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 252 |
| Entropy (8bit): | 2.96847467253794 |
| Encrypted: | false |
| SSDEEP: | 3:kkFklR31fllXlE/+CkJdllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yR9l1LlN:kKCR5liBAIdQZV7Qrl5 |
| MD5: | 8B5B3FD54D39A3B492C7ADCFFAA709ED |
| SHA1: | 63158D1BEAE722B6A3996885C29C604ABCC1B7EE |
| SHA-256: | C1FB6B3AC300A0FF6F654F684BE82F838676700ED56719848587E329D167C31C |
| SHA-512: | C15D22D929BB610BE272CD68D713E7F23BA2480223818C04F88D474EDE7680B974BB4CCC869D7269B9E006A78397E38F530A1A066564FA78ACDDF2E3D3A5C34 |
| Malicious: | false |
| Reputation: | low |
| Preview: | p..... ....`..... ..b..(..... .....[..^.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.c.4.8.0<br>.c.7.c.5.2.f.8.0."... |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PC[1].txt |
|---|

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\PC[1].txt | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | downloaded |
| Size (bytes): | 659456 |
| Entropy (8bit): | 6.648738100237886 |
| Encrypted: | false |
| SSDEEP: | 6144:ie7tkcyarn5KfNZCM2RG+zcwxOVbcEkXd5+d/T7xvoldaoAxKiYe1SvA5UamZ6vh:XFn5W8M4GSYbcb/+V7B+AcigemZ6Xd |
| MD5: | 5688C69C4379841EEE42DCAEC2DBF55A |
| SHA1: | 09A30EC730D1FDF77E80F6D31AA4D810E36B1C44 |
| SHA-256: | 62801897AE3411A8F144F2F7290AD2133AD0895F4F1550922DCA9C6F4B9E8114 |
| SHA-512: | 1CEE75D6FFDC9A1E9E903672C83A7E042E9A6A34D42B156BD11A6ED215A82FE336E86158892A6EE129239F52F22CCFE19062D8668C6B9BE5027775BD1942417 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 22% |
| Reputation: | low |
| IE Cache URL: | http://https://offlineclubz.com/PC.txt |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....37B.....~'... ...@....@.. .....<br>..`.....$'..W....@.....`.....  .....  ..H.....text.....  .....  ..`.rsrc.....@.....@..@.rel<br>oc.....`.....@..B.....`'.....H.....\.....LY..z-.....#Y./..U.[P..c.Q..q<z.....\..k.A..4r..CTd..41n.8.[z..,.4k...f...[....v;+ /...z.p.r..?...ql..<br>.Dy9.V..PA..h..c$....o&.tA.6@.!.bo..../.f).a(.....x.L.Z.....6@.....EM$.7^?.0.w.2O.....C.R...fc...A.>q..P2...aBZ..&o.p7.RS@<.>.TO6!;..*.....Zn.G.s.....r...j....hi.;....B..T..<br>Pn.../@!..o.(...d0.'D:....pu.v...^...T..c....B....G0.K}Y.....ic@....R..d0q..Q.xn.BR...._8.&V...h2...[./.[.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2TE7JJq[1].htm | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | HTML document, ASCII text |
| Category: | dropped |
| Size (bytes): | 118 |
| Entropy (8bit): | 4.5727834342595335 |
| Encrypted: | false |
| SSDEEP: | 3:qVvzLURODccZ/vXbvx9nDylVbeSkHslkFSXbKFvNGb:qFzLIeco3XLx92lReNsIMSLWQb |
| MD5: | 8966664618E37682868AB0D64BEBEBFE |
| SHA1: | 38FCE0D612CDEFBE2F68194AC0D38BE6FB6D3819 |
| SHA-256: | A61F7F7C08995E9DF78299E9C8E65EA7FB97639B3DDF6F32B49DAADD155B8D4C |
| SHA-512: | 8D68BA78CDF5997D9B95D14C70106994AE8C7F2AB02B9F528461F1DF84B7D26AF7BF304056746369D5D168E857182E126F2223EFB9321ACA8E3C75217952DAA8 |
| Malicious: | false |
| Preview: | <html>.<head><title>Bitly</title></head>.<body><a href="https://offlineclubz.com/PC.txt">moved here</a></body>.</html> |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0863C5D3-5908-4917-8F28-8909E0160183}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 2150792 |
| Entropy (8bit): | 4.154182985075007 |
| Encrypted: | false |
| SSDEEP: | 49152:y6ugLOlOuO0O0OBwuOu8uiuKuOuFuZuOuOwzuOuN9OuOoSuOugbq:y6ugLOlOuO0O0OBwuOu8uiuKuOuFuZuA |
| MD5: | 49CA5D1741FDA53C2894B360D1A8D648 |
| SHA1: | 44629C7D28BF1FB4087E0FB72492D2AC083C98F7 |
| SHA-256: | 4E6AE2AA54440C99F7814B49065F3CEE5742EBF6FB019677E2EFBD39958EE19B |
| SHA-512: | 007A71A497CACD348E6490E7BC627EF6CB237AB9041127EF50F52BE985721D4BF038E6B227A324E0C5E658C04B4EB39200904A7B1FC748011D284445EAEAE328 |
| Malicious: | false |
| Preview: | ..@.a.W.B.N.Z.v.a.u.7.K.A.p.V.5.Z.b.@.-.A.d.V.7.o.Z.3.o.9.t.P.U.M.i.Q.O.<.e.h.&.&.8._.M.-.C._.C.C.-.-._.-.s.,.6.5.>.9.0.0.0.8.6.$.C.v.>.I.t.=.i.9.|.:.%.a.P.d._.>.G.n.3.#.<br>b.m.%.;.=...0.3.+.v.U.~.7...4.H.g.H.m.?.?._.W.~.5.+.T.f.I.?.n.M.[.T.M.2.7.R.w.U.D.^.:.e.].f.s.E.&.Q.k.P.0.?.G.N.D.?.v.R.6.K.P.[.H.I.C.n.9.B.i.P.s.R.^.?.].?.E.a.b.P.x.?.u.<br>X.t.:.N.'.z.^.3.f.w.?.!.K.W.#.c.F.d.%.&.V.5.i.?.I.b.K.[.V.~.r.v.W.a.*.w.E.a.9.k.0.t.N.3.:.V.9.3.Z.?.V.].&.J.Z.0.L.A.E.6.o.>.i.p.F.f.n._.m.Q.Y.#.1.e.P.9.r.#.'.[.z.p.w.X.2.4.$.N.A.R.<br>k.D.V.C.|.6.L.5.y.1.^.~.Q.I.6.q.T.m.>.x.I.g.B.R.G.:.f.L.[.i.0.a.*.V.$.U.r.y.h.r.y.].O.f.F.8.Y.n.y.L.I.a.T.I.I.E.C.E.?.:.b.'._.Q.A.p.H.?.d.I.'.2.F.k.:.W.S.3.L.g.7.^.u.!.|.Z.G.g.M.8.<br>S.m.2.j.P.z.B.?.f.x.1.d.K.M.L.*.V.&.m.].].g.?.x.Y.k.m.I.T.8.j.8.&.2.T.u.'.3.U.h.U.U.Y.w.#.e.^.i.y.N.D.X.=.Z...].u.E.K.$.M.>.#.4.O.>.u.p.>.y.*.z.v.E.0.0.I.d.+.>.2.E.r.G.5.<br>L.%.r.%.h.A.?.t.p.V.b.q.2.i._._.Z.p.'.e.m.9.?.7.W.@.Q.T.R.K.I.j.6.'.D.M.D.8.t.y...G.G.*.Z.K.n.?.A.J.c.w.r.9.S.j.^.*.s.3.*.!.c.e.N. |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{248C44A0-30CA-4646-ACFF-79FC9E14ADCB}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1024 |
| Entropy (8bit): | 0.05390218305374581 |
| Encrypted: | false |
| SSDEEP: | 3:ol3lYdn:4Wn |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{248C44A0-30CA-4646-ACFF-79FC9E14ADCB}.tmp | |
|---|---|
| MD5: | 5D4D94EE7E06BBB0AF9584119797B23A |
| SHA1: | DBB111419C704F116EFA8E72471DD83E86E49677 |
| SHA-256: | 4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1 |
| SHA-512: | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4 |
| Malicious: | false |
| Preview: | ..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C2D3EB9C-AB70-4784-8852-5C03B64EE05D}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1536 |
| Entropy (8bit): | 1.3586208805849456 |
| Encrypted: | false |
| SSDEEP: | 3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbv:liiiiiiiifdLloZQc8++lsJe1Mzon |
| MD5: | 074A6EF7D45528608B5D3050054D2C36 |
| SHA1: | FA0468DB929013612B7B3B7C01DED8003CAF3D39 |
| SHA-256: | 28BAF8E05009CC690F7B69EECEB57881D52323E6A9412B10A16F6EBD8A9A8C05 |
| SHA-512: | DC248B1A54330C0574CB95C9E96C7095562FA9AB9673403FBA8377ACB37035A8448DB3113E7363B28C9A9C2D22C7EA52BC6833739B8801F39E6A7E3027AF994E |
| Malicious: | false |
| Preview: | ..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... ..... |

| C:\Users\user\AppData\Local\Temp\CabAEF5.tmp | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | Microsoft Cabinet archive data, 60080 bytes, 1 file |
| Category: | dropped |
| Size (bytes): | 60080 |
| Entropy (8bit): | **7.995256720209506** |
| Encrypted: | **true** |
| SSDEEP: | 768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4 |
| MD5: | 6045BACCF49E1EBA0E674945311A06E6 |
| SHA1: | 379C6234849EECEDE26FAD192C2EE59E0F0221CB |
| SHA-256: | 65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58 |
| SHA-512: | DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB |
| Malicious: | false |
| Preview: | MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|||[.w.M.!<-.}%.C<tDX5\s._..l..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F. |

| C:\Users\user\AppData\Local\Temp\RegAsm.exe | |
|---|---|
| Process: | C:\Users\Public\098765.exe |
| File Type: | PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 64672 |
| Entropy (8bit): | 6.033474133573561 |
| Encrypted: | false |
| SSDEEP: | 768:PedoViadPL1DI9WzutSjeJan8dBhF541kE6Iq8HaVxlYDKz4yqibwEBbr:XiaFJkobMa8dBXG2zbVUDKz4yq3EBbr |
| MD5: | ADF76F395D5A0ECBBF005390B73C3FD2 |
| SHA1: | 017801B7EBD2CC0E1151EEBEC14630DBAEE48229 |
| SHA-256: | 5FF87E563B2DF09E94E17C82741D9A43AED2F214643DC067232916FAE4B35417 |
| SHA-512: | 9670AC5A10719FA312336B790EAD713D78A9999DB236AD0841A32CD689559B9F5F8469E3AF93400F1BE5BAF2B3723574F16EA554C2AAF638734FFF806F18DB2B |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Metadefender, Detection: 0%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |

| C:\Users\user\AppData\Local\Temp\RegAsm.exe | |
|---|---|
| Joe Sandbox View: | • Filename: Ref 0180066743.xlsx, Detection: malicious, Browse<br>• Filename: Purchase Order Price List.xlsx, Detection: malicious, Browse<br>• Filename: Quote QU038097.doc, Detection: malicious, Browse<br>• Filename: 6Cprm97UTl.xls, Detection: malicious, Browse<br>• Filename: Payment_Confirmation_Slip.xlsx, Detection: malicious, Browse<br>• Filename: Overdue Invoice.xlsx, Detection: malicious, Browse<br>• Filename: Quotation.xlsx, Detection: malicious, Browse<br>• Filename: ENCLOSE ORDER LIST.xlsx, Detection: malicious, Browse<br>• Filename: PO INV 195167 & 195324.xlsx, Detection: malicious, Browse<br>• Filename: Bank letter.xlsx, Detection: malicious, Browse<br>• Filename: Quotation.xlsx, Detection: malicious, Browse<br>• Filename: PO 19030004.xlsx, Detection: malicious, Browse<br>• Filename: New PO PO20.xlsx, Detection: malicious, Browse<br>• Filename: ORDER LIST.xlsx, Detection: malicious, Browse<br>• Filename: RFQ 00112.xlsx, Detection: malicious, Browse<br>• Filename: inquiry.xlsx, Detection: malicious, Browse |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&.W.....0..... ........@.. ..... .....k.... .`.....O.....8.....>..... ..... ..H.....text..... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....H.....A..`p.....~P...-.r...p.....(....(....s.....P...*..0.."........(.....-.r...p.rI..p(....s....z.*...0.....(....~P.....o.....*.. (....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.;...}S.....i.>...}T.....i.>...}U.....+m...(....o.....r]..p.o ...,..{T.....{U.....o!....+(.ra..p.o ...,..{T..... |

| C:\Users\user\AppData\Local\Temp\TarAEF6.tmp | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 156885 |
| Entropy (8bit): | 6.30972017530066 |
| Encrypted: | false |
| SSDEEP: | 1536:NlR6c79JjgCyrYBWsWimp4Ydm6Caku2SWsz0OD8reJgMnl3XlMuGmO:N2UJcCyZfdmoku2SL3kMnBGuzO |
| MD5: | 9BE376D85B319264740EF583F548B72A |
| SHA1: | 6C6416CBC51AAC89A21A529695A8FCD3AD5E6B85 |
| SHA-256: | 07FDF8BC502E6BB4CF6AE214694F45C54A53228FC2002B2F17C9A2EF64EB76F6 |
| SHA-512: | 8AFC5D0D046E8B410EC1D29E2E16FB00CD92F8822D678AA0EE2A57098E05F2A0E165858347F035AE593B62BF195802CB6F9A5F92670041E1828669987CEEC7DE |
| Malicious: | false |
| Preview: | 0..d...*.H.....d.0..d....1.0...`.H.e.....0..T...+.....7.....T.0..T.0...+.....7.....L.E*u...210519191503Z0...+.....0..T.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o |

| C:\Users\user\AppData\Local\Temp\tmp7790.tmp | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1307 |
| Entropy (8bit): | 5.10141182324719 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Wa5xtn:cbk4oL600QydbQxlYODOLedq39a5j |
| MD5: | 0110BA0E94E360796104E322DF75DC7B |
| SHA1: | 2BB7D2336F5FF60FD081D548CB4FD2ACB1DFF02C |
| SHA-256: | 967AB39BFA0491BC2107EB6BFF58F3C8750C9D1C6EE34B467FE764593E7768CB |
| SHA-512: | FFF636DB45ED48968BF8738E08AE2EAA1AD665BCB081A568C4669F02BB5816918A89E7B60E2BC7D689423A7697D01369C072578377DB13B1B1050CF5FE9CF46 |
| 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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak |

| C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| File Type: | ISO-8859 text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | 3:8Q1t:8Q1t |

| C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat | |
|---|---|
| MD5: | 38A4642F1D21738670A0A97C59F534B8 |
| SHA1: | 00297350A2EC9C0E1D29843C4DDF97C4029F0701 |
| SHA-256: | 667B327299E4A2AFAF51EE5A8566BD177796B84AF410A31B04B6BC5C9B447220 |
| SHA-512: | 9837D7285E4FF71F5CC70EC12CF85ECC3F7EBBC59CC07EA81B22D4A1720E3A80C81419F4EEBB3C18D5F94BF33A467967678BD65A019B9EC36F4BBBDFB521DDF |
| Malicious: | **true** |
| Preview: | .O.5.0.H |

| C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\task.dat | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 44 |
| Entropy (8bit): | 4.24615711897243 |
| Encrypted: | false |
| SSDEEP: | 3:oNXp4E2J5xAl0L4A:oNP23f0L4A |
| MD5: | 5E660472C77DA3439F72326B5DFFB266 |
| SHA1: | AF5C9036F8FFDEE6DDA4F0FCB98FDCBA1C66929F |
| SHA-256: | D4496716123174FC18832BF7C22003B0A1B4D9140FBC672F91EF5687B85A5446 |
| SHA-512: | B7840F8FF63AE79CB828851FAC8AEFA97E97427E1A5A47967A95C42AB2C3163FC1960F7BB3B065B6509648D133DA3AB8AFBA9B5E6F018DB5556E9153679841B0 |
| Malicious: | false |
| Preview: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Updated Order COA.LNK | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Wed Jun 16 18:01:33 2021, length=2676268, window=hide |
| Category: | dropped |
| Size (bytes): | 2098 |
| Entropy (8bit): | 4.559640915747649 |
| Encrypted: | false |
| SSDEEP: | 24:85k/XTd6jFyoFreKZQDv3qadM7dD25k/XTd6jFyoFreKZQDv3qadM7dV:8S/XT0jFJxHZaQh2S/XT0jFJxHZaQ/ |
| MD5: | 1D986D013CAC96F831E9E632B5E3843D |
| SHA1: | 21A72652B7C0A32B4882C4B193AE460B692A1BB3 |
| SHA-256: | 64DCBD0B651A0FE9D4BA4FE4A943EE10C46C28A4281FF737D828042434399F57 |
| SHA-512: | 252EA7098199805AD0F5936E90D3221E3DBE39C901CEA984B4394ED420DD170BFF554A7BDADDBBDE1CF17842C63A86DC15E7C34435C47C1B15663239BD0CCACC |
| Malicious: | false |
| Preview: | L.....F.... ...<f...{..<f...{.... ..b..,.(.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....t.2.,.(..R1. .UPDATE~1.DOC..X.....Q.y.Q.y*...8.....U.p.d.a.t.e.d. .O.r.d.e.r. .C.O.A...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\179605\Users.user\Desktop\Updated Order COA.doc.,.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.U.p.d.a.t.e.d. .O.r.d.e.r. .C.O.A...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....179605.....D_....3N...W...9F.C |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 89 |
| Entropy (8bit): | 4.359207826504001 |
| Encrypted: | false |
| SSDEEP: | 3:M1EEUkLUoVNkLUmX1EEUkLUv:M+E9528E9C |
| MD5: | 49B80095D2558145DCCEEC72D874A816 |
| SHA1: | 931ADA0FE83161BCC2DBB495CF43FBFB1D3EC2DB |
| SHA-256: | 816C4C832C4BE334D7658C2AC92D0F06323212C8CF8FDE5D3FCB21EE23B2D834 |
| SHA-512: | 2CA750205D5B520F37A66DCED0C22D531EA25E779F7F4B056CCEBF02D6E324C5FF77409CF6F43F481CD56B5F072F29CF54C9103CBA6EF530C247707085035D3 |
| Malicious: | false |
| Preview: | [doc]..Updated Order COA.LNK=0..Updated Order COA.LNK=0..[doc]..Updated Order COA.LNK=0.. |

| C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |

| C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm | |
|---|---|
| Size (bytes): | 162 |
| Entropy (8bit): | 2.431160061181642 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l |
| MD5: | 4CDEC46BF4C5E1435E277CB4821D6306 |
| SHA1: | 506F3E77835A2AE504189833D4EF30799A0ACE45 |
| SHA-256: | 39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537 |
| SHA-512: | 7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75 |
| Malicious: | false |
| Preview: | .user.....A.l.b.u.s.....p.....P.....z.....x... |

| C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | Little-endian UTF-16 Unicode text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 2 |
| Entropy (8bit): | 1.0 |
| Encrypted: | false |
| SSDEEP: | 3:Qn:Qn |
| MD5: | F3B25701FE362EC84616A93A45CE9998 |
| SHA1: | D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB |
| SHA-256: | B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209 |
| SHA-512: | 98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4 |
| Malicious: | false |
| Preview: | .. |

| C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WG4KTJBM.txt | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| File Type: | ASCII text |
| Category: | downloaded |
| Size (bytes): | 90 |
| Entropy (8bit): | 4.367513759017689 |
| Encrypted: | false |
| SSDEEP: | 3:jvDiIEKEc2/KHMYi2EWcKvW26YV/n:fiwEP/KHbi2kKvCYV/n |
| MD5: | A8822E64EB6D7DADA85EF5B64BA6AE9D |
| SHA1: | 9678247403B198C7B085E6190D800BA0B719B52B |
| SHA-256: | 9DD9ACB3E005FE39583C889004C06060F8178291BDD68EDF3048643A51E0E300 |
| SHA-512: | F006C0FD1028DF6432B77BC1CD7E10A6BE7A023B5CDA66E137D57CFC71252A1DBFDB619E8E02348049F675A1564B92AC609A2575D84F351B0F8FA1C2FF78E53 |
| Malicious: | false |
| IE Cache URL: | bit.ly/ |
| Preview: | _bit.l5ga1G-ac8a65c983a3f14e72-00e.bit.ly/.1536.1838876416.30928904.1335906363.30892770.*. |

| C:\Users\user\Desktop\~$dated Order COA.doc | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.431160061181642 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVysAiJNGlzgYGwg32LbO/ln:vdsCkWthASq+l |
| MD5: | 4CDEC46BF4C5E1435E277CB4821D6306 |
| SHA1: | 506F3E77835A2AE504189833D4EF30799A0ACE45 |
| SHA-256: | 39A3F2156450758ACBBCB3D8E9461BB4CDD93F41A3EC3A4013F4EB8D2A906537 |
| SHA-512: | 7039ED1E181A8368526A65F6F0D2F70E5BCEBD37BB3BFD8E270BB305F405DB0D843B1CAF6E4E05F6CF1D203A8AA326A1316CDDDD085DD59DB15A82A26E6FA75 |
| Malicious: | false |
| Preview: | .user.....A.l.b.u.s.....p.....P.....z.....x... |

| C:\Users\Public\098765.exe | |
|---|---|
| Process: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |

| C:\Users\Public\098765.exe | |
|---|---|
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | modified |
| Size (bytes): | 659456 |
| Entropy (8bit): | 6.648738100237886 |
| Encrypted: | false |
| SSDEEP: | 6144:ie7tkcyarn5KfNZCM2RG+zcwxOVbcEkXd5+d/T7xvoldaoAxKiYe1SvA5UamZ6vh:XFn5W8M4GSYbcb/+V7B+AcigemZ6Xd |
| MD5: | 5688C69C4379841EEE42DCAEC2DBF55A |
| SHA1: | 09A30EC730D1FDF77E80F6D31AA4D810E36B1C44 |
| SHA-256: | 62801897AE3411A8F144F2F7290AD2133AD0895F4F1550922DCA9C6F4B9E8114 |
| SHA-512: | 1CEE75D6FFDC9A1E9E903672C83A7E042E9A6A34D42B156BD11A6ED215A82FE336E86158892A6EE129239F52F22CCFE19062D8668C6B9BE5027775BD1942417 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 22% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....37B.....~'... ...@....@.. ..... ..`.....$'..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....`'.....H.....\.....LY..z-.....#Y./..U.[P..c.Q..q<z.....\..k.A..4r..CTd..41n.8.[z..,.4k...f...[....v;+ /...z.p.r..?...ql.. .Dy9.V..PA..h..c$....o&.tA.6@.!.bo..../.f).a(.....x.L.Z.....6@.....EM$.7^?.0.w.2O.....C.R...fc...A.>q..P2...aBZ..&o.p7.RS@<.>.TO6!;..*.....Zn.G.s.....r...j....hi.;.....B..T.. Pn.../@!..o.(...d0.'D:....pu.v...^...T..c....B....G0.K}Y.....ic@....R..d0q..Q.xn.BR...._8.&V...h2...[./.[.. |

# Static File Info

## General

| | |
|---|---|
| File type: | Rich Text Format data, unknown version |
| Entropy (8bit): | 5.29364667275501 |
| TrID: | • Rich Text Format (5005/1) 55.56%<br>• Rich Text Format (4004/1) 44.44% |
| File name: | Updated Order COA.doc |
| File size: | 2676268 |
| MD5: | 59f9c2a162cf48fe5819f58b697c107c |
| SHA1: | f8702f19bae3a9f2dd1fca58f6eae3d6e62d4878 |
| SHA256: | 23a865d4a1205be496c45012233d96255c90102e3925da b252d30d9a70f82ba9 |
| SHA512: | 2a992461f865f9d78cf7c183a97e0051914efd0e1921cf0e 9f589546e3c01aabd2c8fae177d0d5a4111629fe2acbecb c8c7540e42bc542fce9e046ac6c0ccf22 |
| SSDEEP: | 24576:sBhBhBhBhBhBhBhBhBhBhBhBhBhBhBhBhBhBh BhBhBhBhBhBhB2SdWnK596WRaSm:v |
| File Content Preview: | {\rtf00529\page63728156246287781@aWBNZvau7KAp V5Zb@-AdV7oZ3o9tPUMiQO<eh&&8_M-C_CC--_-s,65 >900086$Cv>It=i9\|:%aPd_>Gn3#bm%\vLIL;=\lujj67445 8.03.....+vU~7.4HgHm??_W~5+TfI?nM[TM27RwU D^:e]fsE&QkP0?GND?vR6KP[HICn9BiPsR^?]?EabPx? uXt:N'z^3fw?!KW#cFd%&V5i?Ib |

## File Icon

| | |
|---|---|
| Icon Hash: | e4eea2aaa4b4b4a4 |

## Static RTF Info

### Objects

| Id | Start | Format ID | Format | Classname | Datasize | Filename | Sourcepath | Temppath | Exploit |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 00105CB2h | | | | | | | | no |
| 1 | 00105C81h | | | | | | | | no |

# Network Behavior

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jun 16, 2021 12:01:41.736845970 CEST | 192.168.2.22 | 8.8.8.8 | 0x7e45 | Standard query (0) | bit.ly | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:41.790910006 CEST | 192.168.2.22 | 8.8.8.8 | 0x7e45 | Standard query (0) | bit.ly | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.417480946 CEST | 192.168.2.22 | 8.8.8.8 | 0xef41 | Standard query (0) | offlineclubz.com | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.534173012 CEST | 192.168.2.22 | 8.8.8.8 | 0xef41 | Standard query (0) | offlineclubz.com | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.646984100 CEST | 192.168.2.22 | 8.8.8.8 | 0xef41 | Standard query (0) | offlineclubz.com | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:08.136887074 CEST | 192.168.2.22 | 8.8.8.8 | 0xbeb3 | Standard query (0) | wealthybil lionaire.ddns.net | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:08.196099997 CEST | 192.168.2.22 | 8.8.8.8 | 0xbeb3 | Standard query (0) | wealthybil lionaire.ddns.net | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:25.335786104 CEST | 192.168.2.22 | 8.8.8.8 | 0xe42b | Standard query (0) | wealthybil lionaire.ddns.net | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:41.962121010 CEST | 192.168.2.22 | 8.8.8.8 | 0xa0c2 | Standard query (0) | wealthybil lionaire.ddns.net | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jun 16, 2021 12:01:41.790587902 CEST | 8.8.8.8 | 192.168.2.22 | 0x7e45 | No error (0) | bit.ly | | 67.199.248.10 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:41.790587902 CEST | 8.8.8.8 | 192.168.2.22 | 0x7e45 | No error (0) | bit.ly | | 67.199.248.11 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:41.846062899 CEST | 8.8.8.8 | 192.168.2.22 | 0x7e45 | No error (0) | bit.ly | | 67.199.248.10 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:41.846062899 CEST | 8.8.8.8 | 192.168.2.22 | 0x7e45 | No error (0) | bit.ly | | 67.199.248.11 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.533705950 CEST | 8.8.8.8 | 192.168.2.22 | 0xef41 | No error (0) | offlineclubz.com | | 82.221.105.125 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.646461964 CEST | 8.8.8.8 | 192.168.2.22 | 0xef41 | No error (0) | offlineclubz.com | | 82.221.105.125 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:01:42.709249973 CEST | 8.8.8.8 | 192.168.2.22 | 0xef41 | No error (0) | offlineclubz.com | | 82.221.105.125 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:08.195612907 CEST | 8.8.8.8 | 192.168.2.22 | 0xbeb3 | No error (0) | wealthybil lionaire.ddns.net | | 185.140.53.154 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:08.255234957 CEST | 8.8.8.8 | 192.168.2.22 | 0xbeb3 | No error (0) | wealthybil lionaire.ddns.net | | 185.140.53.154 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:25.396533966 CEST | 8.8.8.8 | 192.168.2.22 | 0xe42b | No error (0) | wealthybil lionaire.ddns.net | | 185.140.53.154 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:03:42.022552013 CEST | 8.8.8.8 | 192.168.2.22 | 0xa0c2 | No error (0) | wealthybil lionaire.ddns.net | | 185.140.53.154 | A (IP address) | IN (0x0001) |

## HTTPS Packets

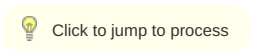
| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| Jun 16, 2021 12:01:41.986649036 CEST | 67.199.248.10 | 443 | 192.168.2.22 | 49167 | CN=bit.ly, O="Bitly, Inc.", L=New York, ST=New York, C=US, SERIALNUMBER=4627013, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US | CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Wed Aug 05 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013 | Tue Aug 10 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 | 771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0 | 7dcce5b76c8b17472d024758970a406b |
| | | | | | CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US | CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US | Tue Oct 22 14:00:00 CEST 2013 | Sun Oct 22 14:00:00 CEST 2028 | | |
| Jun 16, 2021 12:01:42.900809050 CEST | 82.221.105.125 | 443 | 192.168.2.22 | 49168 | CN=offlineclubz.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US | CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. | Wed Jun 16 00:18:52 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021 | Tue Sep 14 00:18:51 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024 | 771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0 | 7dcce5b76c8b17472d024758970a406b |
| | | | | | CN=R3, O=Let's Encrypt, C=US | CN=ISRG Root X1, O=Internet Security Research Group, C=US | Fri Sep 04 02:00:00 CEST 2020 | Mon Sep 15 18:00:00 CEST 2025 | | |
| | | | | | CN=ISRG Root X1, O=Internet Security Research Group, C=US | CN=DST Root CA X3, O=Digital Signature Trust Co. | Wed Jan 20 20:14:03 CET 2021 | Mon Sep 30 20:14:03 CEST 2024 | | |

## Code Manipulations

## Statistics

### Behavior




## System Behavior

### Analysis Process: WINWORD.EXE PID: 1748 Parent PID: 584

#### General

| | |
|---|---|
| Start time: | 12:01:34 |
| Start date: | 16/06/2021 |
| Path: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding |

| | |
|---|---|
| Imagebase: | 0x13ffc0000 |
| File size: | 1424032 bytes |
| MD5 hash: | 95C38D04597050285A18F66039EDB456 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Read**

**Registry Activities** Show Windows behavior

**Key Created**

**Key Value Created**

**Key Value Modified**

## Analysis Process: EQNEDT32.EXE PID: 2624 Parent PID: 584

### General

| | |
|---|---|
| Start time: | 12:01:35 |
| Start date: | 16/06/2021 |
| Path: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding |
| Imagebase: | 0x400000 |
| File size: | 543304 bytes |
| MD5 hash: | A87236E214F6D42A65F5DEDAC816AEC8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**Registry Activities** Show Windows behavior

**Key Created**

## Analysis Process: 098765.exe PID: 2428 Parent PID: 2624

### General

| | |
|---|---|
| Start time: | 12:01:39 |
| Start date: | 16/06/2021 |
| Path: | C:\Users\Public\098765.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\Public\098765.exe |
| Imagebase: | 0xe30000 |
| File size: | 659456 bytes |

| | |
|---|---|
| MD5 hash: | 5688C69C4379841EEE42DCAEC2DBF55A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2121391724.0000000003329000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2121391724.0000000003329000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2121391724.0000000003329000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2121733076.00000000034D6000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2121733076.00000000034D6000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2121733076.00000000034D6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.2121559975.00000000033D8000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.2121559975.00000000033D8000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000002.2121559975.00000000033D8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Antivirus matches: | • Detection: 100%, Joe Sandbox ML<br>• Detection: 22%, ReversingLabs |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: RegAsm.exe PID: 2896 Parent PID: 2428

### General

| | |
|---|---|
| Start time: | 12:01:51 |
| Start date: | 16/06/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| Imagebase: | 0x1f0000 |
| File size: | 64672 bytes |
| MD5 hash: | ADF76F395D5A0ECBBF005390B73C3FD2 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2359788064.0000000003939000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2359788064.0000000003939000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2356733340.0000000000920000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2356733340.0000000000920000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2356733340.0000000000920000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2356337406.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2356337406.0000000000402000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000005.00000002.2356337406.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.2357249695.00000000028F1000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.2356610128.0000000000760000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.2356610128.0000000000760000.00000004.00000001.sdmp, Author: Florian Roth |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |
| Reputation: | moderate |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: schtasks.exe PID: 2456 Parent PID: 2896

### General

| | |
|---|---|
| Start time: | 12:01:56 |
| Start date: | 16/06/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'schtasks.exe' /create /f /tn 'SMTP Service' /xml 'C:\Users\user\AppData\Local\Temp\tmp7790.tmp' |
| Imagebase: | 0x2a0000 |
| File size: | 179712 bytes |
| MD5 hash: | 2003E9B15E1C502B146DAD2E383AC1E3 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: taskeng.exe PID: 2536 Parent PID: 860

### General

| | |
|---|---|
| Start time: | 12:01:58 |
| Start date: | 16/06/2021 |
| Path: | C:\Windows\System32\taskeng.exe |
| Wow64 process (32bit): | false |
| Commandline: | taskeng.exe {6204476F-CB6D-41BF-A018-07A92169AAA2} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] |
| Imagebase: | 0xff3c0000 |
| File size: | 464384 bytes |
| MD5 hash: | 65EA57712340C09B1B0C427B4848AE05 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

Show Windows behavior

#### File Read

### Registry Activities

Show Windows behavior

#### Key Value Created

## Analysis Process: RegAsm.exe PID: 2592 Parent PID: 2536

### General

| | |
|---|---|
| Start time: | 12:01:58 |
| Start date: | 16/06/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\RegAsm.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\RegAsm.exe 0 |
| Imagebase: | 0x1f0000 |
| File size: | 64672 bytes |
| MD5 hash: | ADF76F395D5A0ECBBF005390B73C3FD2 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | moderate |

### File Activities

Show Windows behavior

#### File Read

# Disassembly

## Code Analysis