


**ID:** 448478
**Sample Name:** 5nXX3v5zWn
**Cookbook:** default.jbs
**Time:** 09:33:33
**Date:** 14/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents


Table of Contents 2
Windows Analysis Report 5nXX3v5zWn 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: HawkEye 4
Yara Overview 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Boot Survival: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
Private 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 20
General 20
File Icon 20
Static PE Info 21
General 21
Entrypoint Preview 21
Data Directories 21
Sections 21
Resources 21
Imports 21
Version Infos 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
SMTP Packets 22
Code Manipulations 23
Statistics 23
Behavior 23

System Behavior 23
Analysis Process: 5nXX3v5zWn.exe PID: 3440 Parent PID: 5584 23
General 23
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Analysis Process: powershell.exe PID: 4116 Parent PID: 3440 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Analysis Process: conhost.exe PID: 3876 Parent PID: 4116 24
General 24
Analysis Process: powershell.exe PID: 5796 Parent PID: 3440 24
General 24
File Activities 25
File Created 25
File Deleted 25
File Written 25
File Read 25
Analysis Process: conhost.exe PID: 592 Parent PID: 5796 25
General 25
Analysis Process: schtasks.exe PID: 4420 Parent PID: 3440 25
General 25
File Activities 25
File Read 25
Analysis Process: conhost.exe PID: 5620 Parent PID: 4420 25
General 25
Analysis Process: powershell.exe PID: 2396 Parent PID: 3440 26
General 26
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 26
Analysis Process: 5nXX3v5zWn.exe PID: 5712 Parent PID: 3440 26
General 26
Analysis Process: conhost.exe PID: 2428 Parent PID: 2396 27
General 27
Analysis Process: 5nXX3v5zWn.exe PID: 3708 Parent PID: 3440 27
General 27
Analysis Process: vbc.exe PID: 2440 Parent PID: 3708 27
General 27
Analysis Process: vbc.exe PID: 5356 Parent PID: 3708 27
General 27
Analysis Process: WindowsUpdate.exe PID: 5096 Parent PID: 3388 28
General 28
Analysis Process: WindowsUpdate.exe PID: 3412 Parent PID: 3388 28
General 28
Disassembly 28
Code Analysis 28

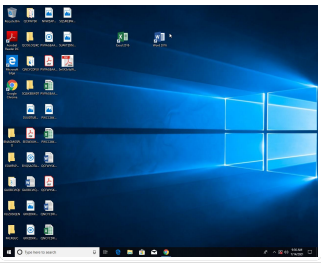
# Windows Analysis Report 5nXX3v5zWn

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 5nXX3v5zWn (renamed file extension from none to exe) |
| Analysis ID: | 448478 |
| MD5: | e35a0bdb66b37b.. |
| SHA1: | 42d31ffa8a8a38d.. |
| SHA256: | 4d16ac850f443e6. |
| Tags: | 32 exe |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

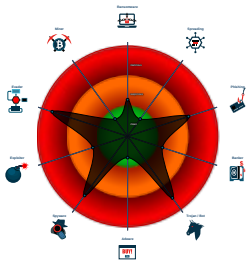
HawkEye
MailPassView

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

### Signatures

- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Adds a directory exclusion to Windo…
- Changes the view of files in windows…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Sample uses process hollowing tech…
- Sigma detected: Powershell Defende…

### Classification



## Process Tree

- **System is w10x64**
- 5nXX3v5zWn.exe (PID: 3440 cmdline: 'C:\Users\user\Desktop\5nXX3v5zWn.exe' MD5: E35A0BDB66B37B80C51A1559058E326B)
  - powershell.exe (PID: 4116 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\5nXX3v5zWn.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5796 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4420 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\egGZqtIOrEmq' /XML 'C:\Users\user\AppData\Local\Temp\tmpA9C5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2396 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 5nXX3v5zWn.exe (PID: 5712 cmdline: C:\Users\user\Desktop\5nXX3v5zWn.exe MD5: E35A0BDB66B37B80C51A1559058E326B)
  - 5nXX3v5zWn.exe (PID: 3708 cmdline: C:\Users\user\Desktop\5nXX3v5zWn.exe MD5: E35A0BDB66B37B80C51A1559058E326B)
    - vbc.exe (PID: 2440 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5356 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- WindowsUpdate.exe (PID: 5096 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: E35A0BDB66B37B80C51A1559058E326B)
- WindowsUpdate.exe (PID: 3412 cmdline: 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' MD5: E35A0BDB66B37B80C51A1559058E326B)
- **cleanup**

## Malware Configuration

### Threatname: HawkEye

```
{
  "Modules": [
    "mailpv",
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


## Yara Overview

## Sigma Overview

### System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

## Jbx 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

Machine Learning detection for dropped file

Machine Learning detection for sample

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

Yara detected HawkEye Keylogger

### System Summary:

Malicious sample detected (through community Yara rule)

### Boot Survival:

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

### Hooking and other Techniques for Hiding and Protection:

Changes the view of files in windows explorer (hidden files and folders)

### Malware Analysis System Evasion:

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

## HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Sample uses process hollowing technique

## Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Yara detected WebBrowserPassView password recovery tool

## Remote Access Functionality:

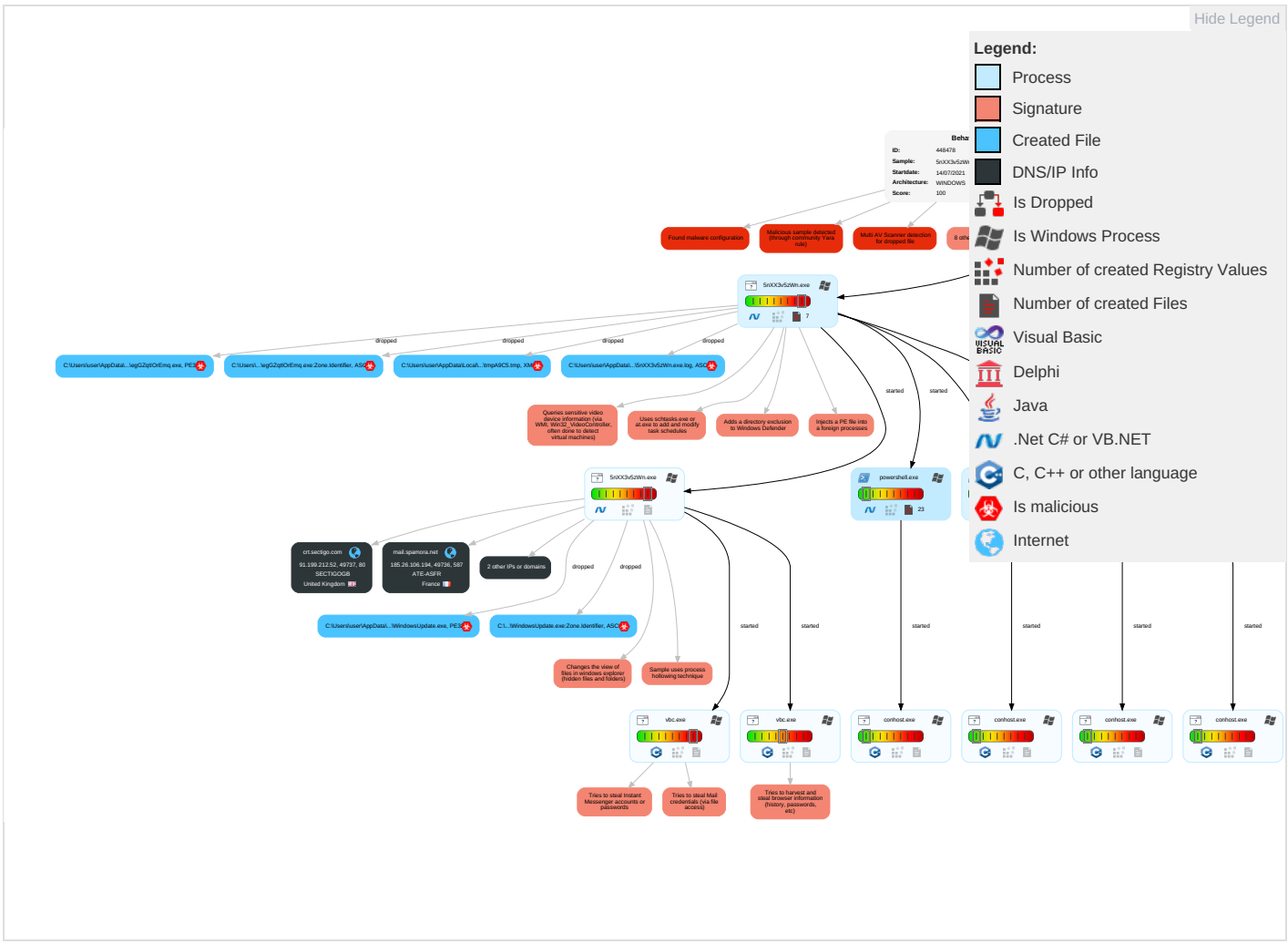
Detected HawkEye Rat

Yara detected HawkEye Keylogger

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration |
|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 1 2 1 | DLL Side-Loading 1 | DLL Side-Loading 1 | Disable or Modify Tools 1 1 | OS Credential Dumping 1 | System Time Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium |
| Default Accounts | Native API 1 | Application Shimming 1 | Application Shimming 1 | Deobfuscate/Decode Files or Information 1 | Credentials in Registry 1 | File and Directory Discovery 2 | Remote Desktop Protocol | Data from Local System 1 | Exfiltration Over Bluetooth |
| Domain Accounts | Shared Modules 1 | Scheduled Task/Job 1 | Process Injection 2 1 2 | Obfuscated Files or Information 4 | Credentials In Files 1 | System Information Discovery 1 9 | SMB/Windows Admin Shares | Email Collection 1 | Automated Exfiltration |
| Local Accounts | Scheduled Task/Job 1 | Registry Run Keys / Startup Folder 1 | Scheduled Task/Job 1 | Software Packing 3 | NTDS | Query Registry 1 | Distributed Component Object Model | Clipboard Data 1 | Scheduled Transfer |
| Cloud Accounts | Cron | Network Logon Script | Registry Run Keys / Startup Folder 1 | DLL Side-Loading 1 | LSA Secrets | Security Software Discovery 2 5 1 | SSH | Keylogging | Data Transfer Size Limits |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Masquerading 1 | Cached Domain Credentials | Virtualization/Sandbox Evasion 1 5 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Modify Registry 1 | DCSync | Process Discovery 4 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Virtualization/Sandbox Evasion 1 5 1 | Proc Filesystem | Application Window Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Process Injection 2 1 2 | /etc/passwd and /etc/shadow | Remote System Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol |
| 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 |

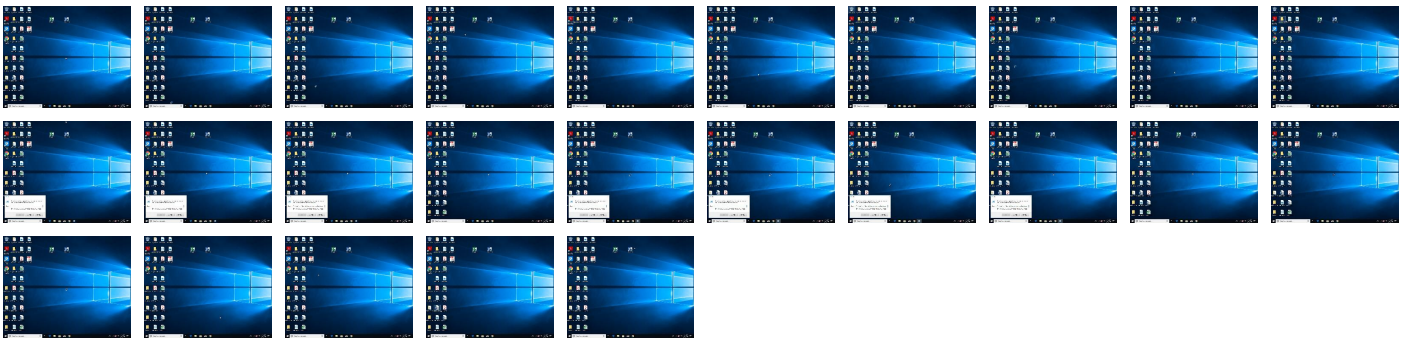
# Behavior Graph




## 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 |
|---|---|---|---|---|
| 5nXX3v5zWn.exe | 46% | Virustotal | | Browse |
| 5nXX3v5zWn.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Roaming\WindowsUpdate.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Roaming\WindowsUpdate.exe | 43% | ReversingLabs | ByteCode-MSIL.Trojan.AgentTesla | |
| C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe | 43% | ReversingLabs | ByteCode-MSIL.Trojan.AgentTesla | |

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 29.2.vbc.exe.400000.0.unpack | 100% | Avira | HEUR/AGEN.1125438 | | Download File |
| 17.2.5nXX3v5zWn.exe.400000.0.unpack | 100% | Avira | TR/AD.MExecute.Izrac | | Download File |
| 17.2.5nXX3v5zWn.exe.400000.0.unpack | 100% | Avira | SPR/Tool.MailPassView.473 | | Download File |

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| mail.spamora.net | 1% | Virustotal | | Browse |
| crt.sectigo.com | 1% | Virustotal | | Browse |
| 231.29.2.0.in-addr.arpa | 0% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://https://contoso.com/License | 0% | URL Reputation | safe | |
| http://https://contoso.com/License | 0% | URL Reputation | safe | |
| http://https://contoso.com/License | 0% | URL Reputation | safe | |
| http://https://contoso.com/License | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt5= | 0% | Avira URL Cloud | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.com | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.com | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.com | 0% | URL Reputation | safe | |
| http://www.typography.netD | 0% | URL Reputation | safe | |
| http://www.typography.netD | 0% | URL Reputation | safe | |
| http://www.typography.netD | 0% | URL Reputation | safe | |
| http://fontfabrik.comq | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.comas | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn/cThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/cThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/cThe | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://https://contoso.com/ | 0% | URL Reputation | safe | |
| http://https://contoso.com/ | 0% | URL Reputation | safe | |
| http://https://contoso.com/ | 0% | URL Reputation | safe | |
| http://mail.spamora.net | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0# | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0# | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0# | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://www.fontbureau.comF | 0% | URL Reputation | safe | |
| http://https://sectigo.com/CPS0 | 0% | URL Reputation | safe | |
| http://https://sectigo.com/CPS0 | 0% | URL Reputation | safe | |
| http://https://sectigo.com/CPS0 | 0% | URL Reputation | safe | |
| http://www.fonts.comc | 0% | URL Reputation | safe | |
| http://www.fonts.comc | 0% | URL Reputation | safe | |
| http://www.fonts.comc | 0% | URL Reputation | safe | |
| http://pesterbdd.com/images/Pester.png | 0% | URL Reputation | safe | |
| http://pesterbdd.com/images/Pester.png | 0% | URL Reputation | safe | |
| http://pesterbdd.com/images/Pester.png | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://go.micro | 0% | URL Reputation | safe | |
| http://https://go.micro | 0% | URL Reputation | safe | |
| http://https://go.micro | 0% | URL Reputation | safe | |
| http://www.tiro.comt.j | 0% | Avira URL Cloud | safe | |
| http://https://contoso.com/Icon | 0% | URL Reputation | safe | |
| http://https://contoso.com/Icon | 0% | URL Reputation | safe | |
| http://https://contoso.com/Icon | 0% | URL Reputation | safe | |
| http://www.tiro.comtn | 0% | Avira URL Cloud | safe | |
| http://www.fontbureau.come.com | 0% | URL Reputation | safe | |
| http://www.fontbureau.come.com | 0% | URL Reputation | safe | |
| http://www.fontbureau.come.com | 0% | URL Reputation | safe | |
| http://en.w | 0% | URL Reputation | safe | |
| http://en.w | 0% | URL Reputation | safe | |
| http://en.w | 0% | URL Reputation | safe | |
| http://ocsp.sectigo.com0% | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://https://go.micro8 | 0% | Avira URL Cloud | safe | |
| http://pesterbdd.com/images/Pester.pngH | 0% | Avira URL Cloud | safe | |
| http://www.microsoft.co_ | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| mail.spamora.net | 185.26.106.194 | true | false | • 1%, Virustotal, Browse | unknown |
| crt.sectigo.com | 91.199.212.52 | true | false | • 1%, Virustotal, Browse | unknown |
| 231.29.2.0.in-addr.arpa | unknown | unknown | false | • 0%, Virustotal, Browse | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 91.199.212.52 | crt.sectigo.com | United Kingdom |  | 48447 | SECTIGOGB | false |
| 185.26.106.194 | mail.spamora.net | France |  | 24935 | ATE-ASFR | false |

## Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 448478 |

| | |
|---|---|
| Start date: | 14.07.2021 |
| Start time: | 09:33:33 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 17m 35s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 5nXX3v5zWn (renamed file extension from none to exe) |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 39 |
| 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.phis.troj.spyw.evad.winEXE@23/23@3/3 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 0.1% (good quality ratio 0.1%)<br>• Quality average: 78.5%<br>• Quality standard deviation: 14.5% |
| 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 |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 09:34:48 | API Interceptor | 24x Sleep call for process: 5nXX3v5zWn.exe modified |
| 09:35:31 | Autostart | Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe |
| 09:35:40 | Autostart | Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe |
| 09:35:52 | API Interceptor | 154x Sleep call for process: powershell.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 91.199.212.52 | H8KFZGwAkB.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | Cmh_Fax-Message-3865.html | Get hash | malicious | Browse | • zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | guesZQt4Yz.exe | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | 2naHs0NOfi.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | 3.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | 3.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | saturo[1].htm | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | cat.exe | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | OW73NJTujh.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | Ak6qIKCI0f.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | DOCUMENT.DLL | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | PNmTyT6wHi.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | DOCUMENT.DLL | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | Documents.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | s.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | s.dll | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| | publiclicense.vbs | Get hash | malicious | Browse | • zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt |
| | 3PL0-MDEO3H-GOF4.html | Get hash | malicious | Browse | • zerossl.crt.sectigo.com/ZeroSSLRSADomainSecureSiteCA.crt |
| | pieChart2.exe | Get hash | malicious | Browse | • crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| mail.spamora.net | Doc_386384934.xlsx | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_38464835648343.xlsx | Get hash | malicious | Browse | • 185.26.106.194 |
| | pfI78aQqmv.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Inquiry.xlsx | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_87654334567.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | PO-4600017931.xlsx | Get hash | malicious | Browse | • 185.26.106.194 |
| | HTOj2DnVlw.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | i7Qs22QuKz.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc.xlsx | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_39563856383648364376383647383654836473836383648363846383.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_987945678.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Ref-2021-05-14.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_38464856384683648364.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Document_printout_copy_34853936483648364393743836384.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | DHL_SHIPMENT_ADDRESS_4495749574946596484658458458,pdf.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | RFQ_384638463936463883683648 34.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_384746836483648363 8463,pdf.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | 938583958330948348430384309 4034.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | SIN_TONG_HWA_TRADING,pdf.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | 9qyjV3QacT.exe | Get hash | malicious | Browse | • 185.26.106.194 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| SECTIGOGB | H8KFZGwAkB.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | Cmh_Fax-Message-3865.html | Get hash | malicious | Browse | • 91.199.212.52 |
| | guesZQt4Yz.exe | Get hash | malicious | Browse | • 91.199.212.52 |
| | 2naHs0NOfi.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | 3.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | 3.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | saturo[1].htm | Get hash | malicious | Browse | • 91.199.212.52 |
| | cat.exe | Get hash | malicious | Browse | • 91.199.212.52 |
| | OW73NJTujh.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | Ak6qIKCI0f.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | DOCUMENT.DLL | Get hash | malicious | Browse | • 91.199.212.52 |
| | PNmTyT6wHi.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | DOCUMENT.DLL | Get hash | malicious | Browse | • 91.199.212.52 |
| | Documents.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | s.dll | Get hash | malicious | Browse | • 91.199.212.52 |
| | s.dll | Get hash | malicious | Browse | • 91.199.212.52 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | publiclicense.vbs | Get hash | malicious | Browse | • 91.199.212.52 |
| | 3PL0-MDEO3H-GOF4.html | Get hash | malicious | Browse | • 91.199.212.52 |
| | pieChart2.exe | Get hash | malicious | Browse | • 91.199.212.52 |
| ATE-ASFR | Doc_386384934.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |
| | Doc_38464835648343.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |
| | pfI78aQqmv.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Inquiry.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |
| | Doc_87654334567.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | PO-4600017931.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |
| | HTOj2DnVlw.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | i7Qs22QuKz.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |
| | Doc_39563856383648364376383647383654836473836483648363846383.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_987945678.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Ref-2021-05-14.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_38464856384683648364.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Document_printout_copy_3485393648364836439374383638 4.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | DHL_SHIPMENT_ADDRESS_4495749574946596484 658458458,pdf.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | DOCUMENT_395849584954.exe | Get hash | malicious | Browse | • 185.26.106.165 |
| | RFQ_384638463936463883683648 34.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Doc_384746836483648363846 3,pdf.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | 938583958330948348430384309 4034.exe | Get hash | malicious | Browse | • 185.26.106.194 |
| | Order_364537463746347485945454.xlsx | Get hash | malicious | Browse | • 185.26.106.165 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\30D802E0E248FEE17AAF4A62594CC75A | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1559 |
| Entropy (8bit): | 7.399832861783252 |
| Encrypted: | false |
| SSDEEP: | 48:B4wgi+96jf8TXJgnXpxi4sVtcTtrdoh+S:Kilq0eZnep |
| MD5: | ADAB5C4DF031FB9299F71ADA7E18F613 |
| SHA1: | 33E4E80807204C2B6182A3A14B591ACD25B5F0DB |
| SHA-256: | 7FA4FF68EC04A99D7528D5085F94907F4D1DD1C5381BACDC832ED5C960214676 |
| SHA-512: | 983B974E459A46EB7A3C8850EC90CC16D3B6D4A1505A5BCDD710C236BAF5AADC58424B192E34A147732E9D436C9FC04D896D8A7700FF349252A57514F588C6A |
| Malicious: | false |
| Preview: | 0...0.....}[Q&.v...t...S..0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...181102000000Z..301231235959Z0..1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Sectigo Limited1705..U....Sectigo RSA Domain Validation Secure Server CA0..."0...*.H.....0.....s3..< ....E..>..?.A.20.l.....-?.M.....b..Hy...N..2%.....P?.L.@*.9.....2A.&.#z. ... .<.Do.u..@.2.....#>...o]Q.j.i.O.ri..Lm.....~... ...7x...4.V.X....d[.7..(h.V...\.....$..0.....z...B.....J.....@..o.BJd..0.....'Z..X.....c.oV...`4.t....._.....n0..j0...U.#..0...Sy.Z.+J.T.....f.0...U.....^.T...w.....a.0...U.....0...U.... ...0.....0...U.%..0...+.....+.....0...U. ..0.0...U. .0...g.....0P..U...I0G0E.C.A.?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v..+.....j0h0?..+.....0..3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%..+.....0. |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 282 |
| Entropy (8bit): | 3.1368173556949515 |

| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 3:kkFklhLpwkNvfllXlE/lPbXx8bqlF8tlije9DZl2i9XYolzlIlMltuN7ANJbZ15z:kK6RNyjXxp9jKFlIaYM2+/LOjA/ |
| MD5: | E46482A591E6E2926D676D36A231C676 |
| SHA1: | 2B62C2F4D903CAFA707B0C2927D378E1FD42BFAF |
| SHA-256: | C4153C1C2F053DFF266A528F81CEBCC2464F1B922F4060D62C141715EA593989 |
| SHA-512: | A8A9E1B516C7C619CD8DA30DFEFC935ED9324A99CF694D7F0A9A4582AD59E2F75720A80C8341D00B1C6F220F6AD326880D0C8028A04FC0A76354CFEDF3E46B3 |
| Malicious: | false |
| Preview: | p..... .....T....x..(..... .....@u.>r..@8.....h.t.t.p.:./.c.r.t...s.e.c.t.i.g.o...c.o.m./.S.e.c.t.i.g.o.R.S.A.D.o.m.a.i.n.V.a.l.i.d.a.t.i.o.n.S.e.c.u.r.e.S.e.r.v.e.r.C.A...c.r.t...".5.b.d.b.9.3.8.0.-.6.1.7."... |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\5nXX3v5zWn.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.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 |
| SHA-256: | 1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427 |
| SHA-512: | C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A |
| Malicious: | **true** |
| 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\ModuleAnalysisCache | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 14734 |
| Entropy (8bit): | 4.993014478972177 |
| Encrypted: | false |
| SSDEEP: | 384:cBVoGIpN6KQkj2Wkjh4iUxx5djHWrxbXX35PYoGib4J:cBV3IpNBQkj2Lh4iUxx5djHWrxbH3RYH |
| MD5: | 456B58368F1597035565FF5661D0A2CE |
| SHA1: | DAC873BF6060F400AB309C040948848CD3019B11 |
| SHA-256: | C1273918592A45B7B6CEABC376395C6701D5C83642143C824BE3E316F9131AA9 |
| SHA-512: | B55743EFD8588B68A89983553BE54FEDBB45F1877513CBA477CBCA36EA2E4D6F6140D61FC342EB326CB0B485E26BAC515B234DCD34909129C4339AAEF18B489 |
| Malicious: | false |
| Preview: | PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module.... |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_102g4eb0.ed4.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 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_102g4eb0.ed4.ps1 | |
|---|---|
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_53yqb03u.w2f.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<br>A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_b3j5vb2e.zhc.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<br>A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mfl5jaou.44l.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<br>A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uyn15uet.dem.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 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uyn15uet.dem.psm1 | |
|---|---|
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A |
| Malicious: | false |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vth45tfl.sdf.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 |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp\holderwb.txt | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.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\Local\Temp\tmpA9C5.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1645 |
| Entropy (8bit): | 5.193776238895854 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBvutn:cbh47TlNQ//rydbz9I3YODOLNdq39I |
| MD5: | 54A7468F56A3A2CD1077D5BC5F5E1CF5 |
| SHA1: | 546DB1F0DA9CBFC04C741F850261FB3862C7E653 |
| SHA-256: | 03E45CEFC430010C346C2A0A872644AA1CC0EA468BC0897ED3D9D764C7DFF8BF |
| SHA-512: | 8C305AA91EA03F18D21BAC550E34A2AF142A8E85667173B6B5C741BBFC09BCF553AB2686313E2AD78A8A971E0D4907E2B2A48D138E144C7D2D8D2911F8D5228A |
| 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\WindowsUpdate.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 1261056 |
| Entropy (8bit): | 7.612252755280688 |

| C:\Users\user\AppData\Roaming\WindowsUpdate.exe | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 24576:J57dzqnUYOCGSfCuuBIRzCa6RMdLAEDv+tgd3gD:hgN97ugl6sUEHd3g |
| MD5: | E35A0BDB66B37B80C51A1559058E326B |
| SHA1: | 42D31FFA8A8A38D5073220550CAE44D3E91BF9D6 |
| SHA-256: | 4D16AC850F443E678E5CDC8C104F9369A97E8347C3A64F3FCE173329072FEE53 |
| SHA-512: | ECF25580F0877CD47826BD23C60C1A871FC8A68C12E300776681B97A55406DD6523981755C477F4E76D09FFC67471E96E784CAE65D1A32F1F023504D26F8E186 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 43% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+..`.....$.....5... .....@.. .....<br>..@.....5..W....@..."..... ..... ..H.....text..... ..... ..`.rsrc...."...@..."..... @..@.rel<br>oc.....<.....@..B.....5.....H.....2.....t.....`.....(....*&..(....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....<br>.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p.....(....s....z..+..s.....~.....<br>(.....o.....(...+..tu....%-.&.+.%(.....o.....&r;..p.. |

| C:\Users\user\AppData\Roaming\WindowsUpdate.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| 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\AppData\Roaming\egGZqtlOrEmq.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 1261056 |
| Entropy (8bit): | 7.612252755280688 |
| Encrypted: | false |
| SSDEEP: | 24576:J57dzqnUYOCGSfCuuBIRzCa6RMdLAEDv+tgd3gD:hgN97ugl6sUEHd3g |
| MD5: | E35A0BDB66B37B80C51A1559058E326B |
| SHA1: | 42D31FFA8A8A38D5073220550CAE44D3E91BF9D6 |
| SHA-256: | 4D16AC850F443E678E5CDC8C104F9369A97E8347C3A64F3FCE173329072FEE53 |
| SHA-512: | ECF25580F0877CD47826BD23C60C1A871FC8A68C12E300776681B97A55406DD6523981755C477F4E76D09FFC67471E96E784CAE65D1A32F1F023504D26F8E186 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 43% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+..`.....$.....5... .....@.. .....<br>..@.....5..W....@..."..... ..... ..H.....text..... ..... ..`.rsrc...."...@..."..... @..@.rel<br>oc.....<.....@..B.....5.....H.....2.....t.....`.....(....*&..(....*...s.....s.....s.....s.....s.....*.0.....~....o.....+..*.0.....<br>.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p.....(....s....z..+..s.....~.....<br>(.....o.....(...+..tu....%-.&.+.%(.....o.....&r;..p.. |

| C:\Users\user\AppData\Roaming\egGZqtlOrEmq.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| 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** |

| C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe:Zone.Identifier | |
|---|---|
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\AppData\Roaming\pid.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 4 |
| Entropy (8bit): | 2.0 |
| Encrypted: | false |
| SSDEEP: | 3:V3:V |
| MD5: | 34FFEB359A192EB8174B6854643CC046 |
| SHA1: | B6356EEB8338BF9C15899584BBB23135B40452E9 |
| SHA-256: | AAF68675C4BEA5600C273F6D4371E8D1B9F383A6DD96DB30D628CF77DD91C09C |
| SHA-512: | 7125DC16314E6314E32BE5A58539CA75B0E7B6C93B5F1F443FD79E991EDBDBA5BD11F8333EF60EB6CD193149339D547DEB837284165D0805FA98BDE473DC532 |
| Malicious: | false |
| Preview: | 3708 |

| C:\Users\user\AppData\Roaming\pidloc.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 37 |
| Entropy (8bit): | 4.378240189894803 |
| Encrypted: | false |
| SSDEEP: | 3:oNWXp5vQzJan:oNWXpFQzJa |
| MD5: | 9B2E0EF287AECA34C538735F6911FF16 |
| SHA1: | 799321AE3A0E0AB5DF00271838F3474413A1E65E |
| SHA-256: | 9624C88E7D3593FBEE0AD1F0260CFA8790B1B9120F0C620965A5C70545B15F48 |
| SHA-512: | 4474C7CE433130E3D2936E541F85DEA3656EE2ADCCD26E4267C9BA4C9A0C0A34FCC186F2AFD67D85941C386678271B958636F2A401961F58DF6437746DAA663 |
| Malicious: | false |
| Preview: | C:\Users\user\Desktop\5nXX3v5zWn.exe |

| C:\Users\user\Documents\20210714\PowerShell_transcript.138727.JIVpCcrj.20210714093452.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): | 830 |
| Entropy (8bit): | 5.332111071096532 |
| Encrypted: | false |
| SSDEEP: | 24:BxSAWyxvBnEx2DOXUWeSunWoHjeTKKjX4CIym1ZJX+Quf:BZWuvhEoO+SZoqDYB1ZUQi |
| MD5: | 94588FD4A32EB364C910B1E6AD32D23B |
| SHA1: | 1DA2A4FCC3BC452A1E7398B5CB45A624E942E216 |
| SHA-256: | E1848E3832F83A9069FE97556CE8EDA2218FF98CEC263E9F20E171015E42AB4D |
| SHA-512: | 69007B309A4DFEDB1E4F61969EEE428CCD276C44BC563B3555A9164531FFC6EBAA8DA15254AF0A9D44C27C7FD1594F4F6FED6BD4CB3D05AA97652ED11F027C 82 |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210714093523..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\5nXX3v5zWn.exe..Process ID: 4116..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: 20210714093523..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\5nXX3v5zWn.exe.. |

| C:\Users\user\Documents\20210714\PowerShell_transcript.138727.fYco6+D0.20210714093453.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): | 850 |
| Entropy (8bit): | 5.377039057069052 |
| Encrypted: | false |
| SSDEEP: | 24:BxSAWIyxvBnEx2DOXUWeSu7+W9HjeTKKjX4CIym1ZJX++u7S:BZWVvhEoO+Sap9qDYB1ZU+aS |
| MD5: | 4EF8EF97D8E4E08A184CD43F7097033C |
| SHA1: | F92F94AFDF384855D165E1BFED84ED7F600E812B |

| C:\Users\user\Documents\20210714\PowerShell_transcript.138727.fYco6+D0.20210714093453.txt | |
|---|---|
| SHA-256: | E613E0385939AD5341FC47B3263DE8607323989F917C1200B141E8E09746700D |
| SHA-512: | 718FFAA99783B53F1BA0381A270C92BDB2E3E065F583B4A2868E0488B6B7A0DD234CE14694DD07D751708EA85745C0A689F16B1A5CE0E4C348D917F2A5F4C16 |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210714093524..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe..Process ID: 5796..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: 20210714093525..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe.. |

| C:\Users\user\Documents\20210714\PowerShell_transcript.138727.oUfNsHgU.20210714093455.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): | 850 |
| Entropy (8bit): | 5.375135860207132 |
| Encrypted: | false |
| SSDEEP: | 24:BxSAWDyxvBnEx2DOXUWeSu7+W4HjeTKKjX4CIym1ZJX+PFu7S:BZWCvhEoO+Sap4qDYB1ZUNaS |
| MD5: | 2C05EFF153AF7A0EAC8540EA6E272E53 |
| SHA1: | C2B06ADB191827F59E9B52DF54FE22DFA8144469 |
| SHA-256: | FD4FEEAE6F18B3D8F1D1430AE723887D80DC4971E8D2E74BEEEC0D25EC637F35 |
| SHA-512: | 900A1FA87F9ED873B99BC9EF95EEECCC4D70EE844467C0E02D145A0CAF4DF77DC1E7B6EC18EFA0C496F1DE6C577F43E7C7B953970E081CF4538C1D76AA3F444 |
| Malicious: | false |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210714093534..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe..Process ID: 2396..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: 20210714093535..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\egGZqtIOrEmq.exe.. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.612252755280688 |
| 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: | 5nXX3v5zWn.exe |
| File size: | 1261056 |
| MD5: | e35a0bdb66b37b80c51a1559058e326b |
| SHA1: | 42d31ffa8a8a38d5073220550cae44d3e91bf9d6 |
| SHA256: | 4d16ac850f443e678e5cdc8c104f9369a97e8347c3a64f3fce173329072fee53 |
| SHA512: | ecf25580f0877cd47826bd23c60c1a871fc8a68c12e300776681b97a55406dd6523981755c477f4e76d09ffc67471e96e784cae65d1a32f1f023504d26f8e186 |
| SSDEEP: | 24576:J57dzqnUYOCGSfCuuBIRzCa6RMdLAEDv+tgd3gD:hgN97ugl6sUEHd3g |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+..`.....$.....5... .....@.. .....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 97194b4a5b6f575b |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x5335fe |
| 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: | 0x60ECE62B [Tue Jul 13 01:02:35 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 | 0x131604 | 0x131800 | False | 0.847971115487 | data | 7.61581587782 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x134000 | 0x2200 | 0x2200 | False | 0.474954044118 | data | 5.89003096224 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x138000 | 0xc | 0x200 | False | 0.041015625 | data | 0.0815394123432 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jul 14, 2021 09:35:22.495374918 CEST | 192.168.2.3 | 8.8.8.8 | 0x1959 | Standard query (0) | 231.29.2.0.in-addr.arpa | PTR (Pointer record) | IN (0x0001) |
| Jul 14, 2021 09:35:52.507955074 CEST | 192.168.2.3 | 8.8.8.8 | 0xca54 | Standard query (0) | mail.spamora.net | A (IP address) | IN (0x0001) |
| Jul 14, 2021 09:35:54.149662018 CEST | 192.168.2.3 | 8.8.8.8 | 0x4c29 | Standard query (0) | crt.sectigo.com | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jul 14, 2021 09:35:22.508961916 CEST | 8.8.8.8 | 192.168.2.3 | 0x1959 | Name error (3) | 231.29.2.0.in-addr.arpa | none | none | PTR (Pointer record) | IN (0x0001) |
| Jul 14, 2021 09:35:52.521961927 CEST | 8.8.8.8 | 192.168.2.3 | 0xca54 | No error (0) | mail.spamora.net | | 185.26.106.194 | A (IP address) | IN (0x0001) |
| Jul 14, 2021 09:35:54.163563967 CEST | 8.8.8.8 | 192.168.2.3 | 0x4c29 | No error (0) | crt.sectigo.com | | 91.199.212.52 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- crt.sectigo.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.3 | 49737 | 91.199.212.52 | 80 | C:\Users\user\Desktop\5nXX3v5zWn.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 14, 2021 09:35:54.279583931 CEST | 5271 | OUT | GET /SectigoRSADomainValidationSecureServerCA.crt HTTP/1.1<br>Connection: Keep-Alive<br>Accept: */*<br>User-Agent: Microsoft-CryptoAPI/10.0<br>Host: crt.sectigo.com |
| Jul 14, 2021 09:35:54.325414896 CEST | 5273 | IN | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Wed, 14 Jul 2021 07:35:54 GMT<br>Content-Type: application/pkix-cert<br>Content-Length: 1559<br>Connection: keep-alive<br>Last-Modified: Fri, 02 Nov 2018 00:00:00 GMT<br>ETag: "5bdb9380-617"<br>X-CCACDN-Mirror-ID: mscrl2<br>Cache-Control: max-age=14400, s-maxage=3600<br>X-CCACDN-Proxy-ID: mcdpinlb6<br>X-Frame-Options: SAMEORIGIN<br>Accept-Ranges: bytes<br>Data Raw: 30 82 06 13 30 82 03 fb a0 03 02 01 02 02 10 7d 5b 51 26 b4 76 ba 11 db 74 16 0b bc 53 0d a7 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00 30 81 88 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 0a 4e 65 77 20 4a 65 72 73 65 79 31 14 30 12 06 03 55 04 07 13 0b 4a 65 72 73 65 79 20 43 69 74 79 31 1e 30 1c 06 03 55 04 0a 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4e 65 74 77 6f 72 6b 31 2e 30 2c 06 03 55 04 03 13 25 55 53 45 52 54 72 75 73 74 20 52 53 41 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d 31 38 31 31 30 32 30 30 30 30 5a 17 0d 33 30 31 32 33 31 32 33 35 39 35 39 5a 30 81 8f 31 0b 30 09 06 03 55 04 06 13 02 47 42 31 1b 30 19 06 03 55 04 08 13 12 47 72 65 61 74 65 72 20 4d 61 6e 63 68 65 73 74 65 72 31 10 30 0e 06 03 55 04 07 13 07 53 61 6c 66 6f 72 64 31 18 30 16 06 03 55 04 0a 13 0f 53 65 63 74 69 67 6f 20 4c 69 6d 69 74 65 64 31 37 30 35 06 03 55 04 03 13 2e 53 65 63 74 69 67 6f 20 52 53 41 20 44 6f 6d 61 69 6e 20 56 61 6c 69 64 61 74 69 6f 6e 20 53 65 63 75 72 65 20 53 65 72 76 65 72 20 43 41 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 d6 73 33 d6 d7 3c 20 d0 00 d2 17 45 b8 d6 3e 07 a2 3f c7 41 ee 32 30 c9 b0 6c fd f4 9f cb 12 98 0f 2d 3f 8d 4d 01 0c 82 0f 17 7f 62 2e e9 b8 48 79 fb 16 83 4e ad d7 32 25 93 b7 07 bf b9 50 3f a9 4c c3 40 2a e9 39 ff d9 81 ca 1f 16 32 41 da 80 26 b9 23 7a 87 20 1e e3 ff 20 9a 3c 95 44 6f 87 75 06 90 40 b4 32 93 16 09 10 08 23 3e d2 dd 87 0f 6f 5d 51 14 6a 0a 69 c5 4f 01 72 69 cf d3 93 4c 6d 04 a0 a3 1b 82 7e b1 9a b9 ed c5 9e c5 37 78 9f 9a 08 34 fb 56 2e 58 c4 09 0e 06 64 5b bc 37 dc f1 9f 28 68 a8 56 b0 92 a3 5c 9f bb 88 98 08 1b 24 1d ab 30 85 ae af b0 2e 9e 7a 9d c1 c0 42 1c e2 02 f0 ea e0 4a d2 ef 90 0e b4 c1 40 16 f0 6f 85 42 4a 64 f7 a4 30 a0 fe bf 2e a3 27 5a 8e 8b 58 b8 ad c3 19 17 84 63 ed 6f 56 fd 83 cb 60 34 c4 74 be e6 9d db e1 e4 e5 ca 0c 5f 15 02 03 01 00 01 a3 82 01 6e 30 82 01 6a 30 1f 06 03 55 1d 23 04 18 30 16 80 14 53 79 bf 5a aa 2b 4a cf 54 80 e1 d8 9b c0 9d f2 b2 03 66 cb 30 1d 06 03 55 1d 0e 04 16 04 14 8d 8c 5e c4 54 ad 8a e1 77 e9 9b f9 9b 05 e1 b8 01 8d 61 e1 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 86 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02 30 1b 06 03 55 1d 20 04 14 30 12 30 06 06 04 55 1d 20 00 30 08 06 06 67 81 0c 01 02 01 30 50 06 03 55 1d 1f 04 49 30 47 30 45 a0 43 a0 41 86 3f 68 74 74 70 3a 2f 2f 63 72 6c 2e 75 73 65 72 74 72 75 73 74 2e 63 6f 6d 2f 55 53 45 52 54 72 75 73 74 52 53 41 43 65 72 74 69 66 69 63 61 74 69 6f 6e 41 75 74 68 6f 72 69 74 79 2e 63 72 6c 30 76 06 08 2b 06 01 05 05 07 01 01 04 6a 30 68 30 3f 06 08 2b 06 01 05 05 07 30 02 86 33 68 74 74 70 3a 2f 2f 63 72 74 2e 75 73 65 72 74 72 75 73 74 2e 63 6f 6d 2f<br>Data Ascii: 00}[Q&vtS0*H010UUS10UNew Jersey10UJersey City10UThe USERTRUST Network1.0,U%USERTrust RSA Certification Authority0181102000000Z301231235959Z010UGB10UGreater Manchester10USalford10USectigo Limited1705U.Sectigo RSA Domain Validation Secure Server CA0"0*H0s3< E>?A20l-?Mb.HyN2%P?L@*92A&#z <Dou@2#>o]QjiOriLm~7x4V.Xd[7(hV\$0.zBJ@oBJd0.'ZXcoV`4t_n0j0U#0SyZ+JTf0U^Twa0U0U00U%0++0U 00U 0g0PUI0G0ECA?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v+j0h0?+03http://crt.usertrust.com/ |

## SMTP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Jul 14, 2021 09:35:52.686177015 CEST | 587 | 49736 | 185.26.106.194 | 192.168.2.3 | 220-mail.spamora.net ESMTP Postfix (Debian/GNU) |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP | Commands |
|---|---|---|---|---|---|
| Jul 14, 2021 09:35:52.693514109 CEST | 49736 | 587 | 192.168.2.3 | 185.26.106.194 | EHLO 138727 |
| Jul 14, 2021 09:35:52.788518906 CEST | 587 | 49736 | 185.26.106.194 | 192.168.2.3 | 220 mail.spamora.net ESMTP Postfix (Debian/GNU) |
| Jul 14, 2021 09:35:52.825865984 CEST | 587 | 49736 | 185.26.106.194 | 192.168.2.3 | 250-mail.spamora.net<br>250-PIPELINING<br>250-SIZE 80000000<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 |
| Jul 14, 2021 09:35:52.826230049 CEST | 49736 | 587 | 192.168.2.3 | 185.26.106.194 | STARTTLS |
| Jul 14, 2021 09:35:52.853914022 CEST | 587 | 49736 | 185.26.106.194 | 192.168.2.3 | 220 2.0.0 Ready to start TLS |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: 5nXX3v5zWn.exe PID: 3440 Parent PID: 5584

#### General

| | |
|---|---|
| Start time: | 09:34:24 |
| Start date: | 14/07/2021 |
| Path: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\5nXX3v5zWn.exe' |
| Imagebase: | 0xe60000 |
| File size: | 1261056 bytes |
| MD5 hash: | E35A0BDB66B37B80C51A1559058E326B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | low |

#### File Activities

Show Windows behavior

##### File Created

##### File Deleted

##### File Written

##### File Read

## Analysis Process: powershell.exe PID: 4116 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:49 |
| Start date: | 14/07/2021 |
| 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\5nXX3v5zWn.exe' |
| Imagebase: | 0x11b0000 |
| 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: 3876 Parent PID: 4116

### General

| | |
|---|---|
| Start time: | 09:34:49 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| 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: powershell.exe PID: 5796 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:49 |
| Start date: | 14/07/2021 |
| 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\AppData\Roaming\egGZqtlOrEmq.exe' |
| Imagebase: | 0x11b0000 |
| 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: 592 Parent PID: 5796

### General

| | |
|---|---|
| Start time: | 09:34:50 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| 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: 4420 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:50 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\egGZqtIOrEmq' /XML 'C:\Users\user\AppData\Local\Temp\tmpA9C5.tmp' |
| Imagebase: | 0x1160000 |
| 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

**File Read**

## Analysis Process: conhost.exe PID: 5620 Parent PID: 4420

### General

| | |
|---|---|
| Start time: | 09:34:51 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| 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: powershell.exe PID: 2396 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:52 |
| Start date: | 14/07/2021 |
| 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\AppData\Roaming\egGZqtlOrEmq.exe' |
| Imagebase: | 0x11b0000 |
| 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: 5nXX3v5zWn.exe PID: 5712 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:53 |
| Start date: | 14/07/2021 |
| Path: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| Imagebase: | 0x330000 |
| File size: | 1261056 bytes |
| MD5 hash: | E35A0BDB66B37B80C51A1559058E326B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: conhost.exe PID: 2428 Parent PID: 2396

### General

| | |
|---|---|
| Start time: | 09:34:53 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff6b2800000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: 5nXX3v5zWn.exe PID: 3708 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 09:34:54 |
| Start date: | 14/07/2021 |
| Path: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\Desktop\5nXX3v5zWn.exe |
| Imagebase: | 0xb50000 |
| File size: | 1261056 bytes |
| MD5 hash: | E35A0BDB66B37B80C51A1559058E326B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

## Analysis Process: vbc.exe PID: 2440 Parent PID: 3708

### General

| | |
|---|---|
| Start time: | 09:35:35 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' |
| Imagebase: | 0x400000 |
| File size: | 1171592 bytes |
| MD5 hash: | C63ED21D5706A527419C9FBD730FFB2E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: vbc.exe PID: 5356 Parent PID: 3708

### General

| | |
|---|---|
| Start time: | 09:35:35 |
| Start date: | 14/07/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' |
| Imagebase: | 0x400000 |
| File size: | 1171592 bytes |
| MD5 hash: | C63ED21D5706A527419C9FBD730FFB2E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: WindowsUpdate.exe PID: 5096 Parent PID: 3388

### General

| | |
|---|---|
| Start time: | 09:35:41 |
| Start date: | 14/07/2021 |
| Path: | C:\Users\user\AppData\Roaming\WindowsUpdate.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' |
| Imagebase: | 0xf90000 |
| File size: | 1261056 bytes |
| MD5 hash: | E35A0BDB66B37B80C51A1559058E326B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Antivirus matches: | • Detection: 100%, Joe Sandbox ML<br>• Detection: 43%, ReversingLabs |

## Analysis Process: WindowsUpdate.exe PID: 3412 Parent PID: 3388

### General

| | |
|---|---|
| Start time: | 09:35:50 |
| Start date: | 14/07/2021 |
| Path: | C:\Users\user\AppData\Roaming\WindowsUpdate.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Roaming\WindowsUpdate.exe' |
| Imagebase: | 0x260000 |
| File size: | 1261056 bytes |
| MD5 hash: | E35A0BDB66B37B80C51A1559058E326B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

# Disassembly

## Code Analysis