


**ID:** 500960
**Sample Name:** dAkJsQr7A9.exe
**Cookbook:** default.jbs
**Time:** 12:33:05
**Date:** 12/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents


Table of Contents 2
Windows Analysis Report dAkJsQr7A9.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
Operating System Destruction: 6
System Summary: 6
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 12
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 24
Rich Headers 24
Data Directories 24
Sections 25
Resources 25
Imports 25
Possible Origin 25
Network Behavior 25
Snort IDS Alerts 25
Network Port Distribution 25
TCP Packets 25
UDP Packets 25

DNS Queries 25
DNS Answers 26
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: dAkJsQr7A9.exe PID: 6308 Parent PID: 3652 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Written 27
File Read 27
Analysis Process: xmjk.pif PID: 6660 Parent PID: 6308 27
General 27
File Activities 29
File Created 29
File Written 29
File Read 29
Registry Activities 29
Key Value Created 29
Analysis Process: RegSvcs.exe PID: 5792 Parent PID: 6660 29
General 29
File Activities 29
File Created 30
File Deleted 30
File Written 30
File Read 30
Registry Activities 30
Key Value Created 30
Analysis Process: schtasks.exe PID: 7124 Parent PID: 5792 30
General 30
File Activities 30
File Read 30
Analysis Process: conhost.exe PID: 6936 Parent PID: 7124 30
General 30
Analysis Process: schtasks.exe PID: 6760 Parent PID: 5792 30
General 30
File Activities 31
File Read 31
Analysis Process: RegSvcs.exe PID: 6312 Parent PID: 664 31
General 31
File Activities 31
File Created 31
File Written 31
File Read 31
Analysis Process: conhost.exe PID: 6580 Parent PID: 6760 31
General 31
Analysis Process: conhost.exe PID: 6560 Parent PID: 6312 32
General 32
Analysis Process: xmjk.pif PID: 6848 Parent PID: 3352 32
General 32
Analysis Process: dhcpmon.exe PID: 7096 Parent PID: 664 32
General 32
File Activities 32
File Created 32
File Written 32
File Read 33
Analysis Process: conhost.exe PID: 7112 Parent PID: 7096 33
General 33
Analysis Process: xmjk.pif PID: 4356 Parent PID: 3352 33
General 33
File Activities 35
File Deleted 35
File Written 35
File Read 35
Analysis Process: wscript.exe PID: 6420 Parent PID: 3352 35
General 35
File Activities 35
Analysis Process: xmjk.pif PID: 4608 Parent PID: 6420 35
General 35
Analysis Process: RegSvcs.exe PID: 5572 Parent PID: 4356 36
General 36
Analysis Process: xmjk.pif PID: 3412 Parent PID: 6420 36
General 36
Disassembly 38
Code Analysis 38

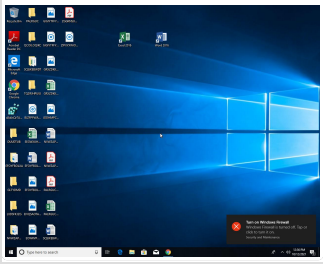
# Windows Analysis Report dAkJsQr7A9.exe

## Overview

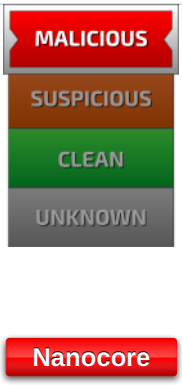
### General Information

| | |
|---|---|
| Sample Name: | dAkJsQr7A9.exe |
| Analysis ID: | 500960 |
| MD5: | b115228fe5e180f.. |
| SHA1: | c242c6a90ae569.. |
| SHA256: | a64c1b956bb79c.. |
| Tags: | exe NanoCore RAT |
| Infos: | |

Most interesting Screenshot:



### Detection



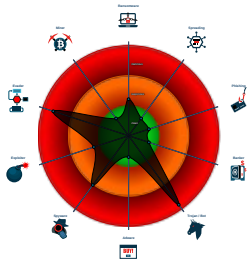

Nanocore

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

### Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Connects to many ports of the same…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add …

### Classification



## Process Tree

- **System is w10x64**
- dAkJsQr7A9.exe (PID: 6308 cmdline: 'C:\Users\user\Desktop\dAkJsQr7A9.exe' MD5: B115228FE5E180F505C081AA829C1A86)
  - xmjk.pif (PID: 6660 cmdline: 'C:\Users\user\31956653\xmjk.pif' thjfdg.xcp MD5: 279DAE7236F5F2488A4BACDE6027F730)
    - RegSvcs.exe (PID: 5792 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 7124 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7982.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6760 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp7CDE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6312 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- xmjk.pif (PID: 6848 cmdline: 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp MD5: 279DAE7236F5F2488A4BACDE6027F730)
- dhcpmon.exe (PID: 7096 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- xmjk.pif (PID: 4356 cmdline: 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp MD5: 279DAE7236F5F2488A4BACDE6027F730)
  - RegSvcs.exe (PID: 5572 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 6420 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\31956653\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - xmjk.pif (PID: 4608 cmdline: 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp MD5: 279DAE7236F5F2488A4BACDE6027F730)
  - xmjk.pif (PID: 3412 cmdline: 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp MD5: 279DAE7236F5F2488A4BACDE6027F730)
    - RegSvcs.exe (PID: 6788 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 6232 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xf9ed:$x1: NanoCore.ClientPluginHost<br>• 0xfa2a:$x2: IClientNetworkHost<br>• 0x1355d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xf755:$a: NanoCore<br>• 0xf765:$a: NanoCore<br>• 0xf999:$a: NanoCore<br>• 0xf9ad:$a: NanoCore<br>• 0xf9ed:$a: NanoCore<br>• 0xf7b4:$b: ClientPlugin<br>• 0xf9b6:$b: ClientPlugin<br>• 0xf9f6:$b: ClientPlugin<br>• 0xf8db:$c: ProjectData<br>• 0x102e2:$d: DESCrypto<br>• 0x17cae:$e: KeepAlive<br>• 0x15c9c:$g: LogClientMessage<br>• 0x11e97:$i: get_Connected<br>• 0x10618:$j: #=q<br>• 0x10648:$j: #=q<br>• 0x10664:$j: #=q<br>• 0x10694:$j: #=q<br>• 0x106b0:$j: #=q<br>• 0x106cc:$j: #=q<br>• 0x106fc:$j: #=q<br>• 0x10718:$j: #=q |
| 00000004.00000003.350063292.000000000443 1000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xf9dd:$x1: NanoCore.ClientPluginHost<br>• 0x441e5:$x1: NanoCore.ClientPluginHost<br>• 0xfa1a:$x2: IClientNetworkHost<br>• 0x44222:$x2: IClientNetworkHost<br>• 0x1354d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe<br>• 0x47d55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000004.00000003.350063292.000000000443 1000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| Click to see the 181 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 20.3.xmjk.pif.4d3c088.5.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x1018d:$x1: NanoCore.ClientPluginHost<br>• 0x101ca:$x2: IClientNetworkHost<br>• 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 20.3.xmjk.pif.4d3c088.5.raw.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xff05:$x1: NanoCore Client.exe<br>• 0x1018d:$x2: NanoCore.ClientPluginHost<br>• 0x117c6:$s1: PluginCommand<br>• 0x117ba:$s2: FileCommand<br>• 0x1266b:$s3: PipeExists<br>• 0x18422:$s4: PipeCreated<br>• 0x101b7:$s5: IClientLoggingHost |
| 20.3.xmjk.pif.4d3c088.5.raw.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 20.3.xmjk.pif.4d3c088.5.raw.unpack | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xfef5:$a: NanoCore<br>• 0xff05:$a: NanoCore<br>• 0x10139:$a: NanoCore<br>• 0x1014d:$a: NanoCore<br>• 0x1018d:$a: NanoCore<br>• 0xff54:$b: ClientPlugin<br>• 0x10156:$b: ClientPlugin<br>• 0x10196:$b: ClientPlugin<br>• 0x1007b:$c: ProjectData<br>• 0x10a82:$d: DESCrypto<br>• 0x1844e:$e: KeepAlive<br>• 0x1643c:$g: LogClientMessage<br>• 0x12637:$i: get_Connected<br>• 0x10db8:$j: #=q<br>• 0x10de8:$j: #=q<br>• 0x10e04:$j: #=q<br>• 0x10e34:$j: #=q<br>• 0x10e50:$j: #=q<br>• 0x10e6c:$j: #=q<br>• 0x10e9c:$j: #=q<br>• 0x10eb8:$j: #=q |
| 25.2.RegSvcs.exe.34d9650.3.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x42a6:$x1: NanoCore.ClientPluginHost |
| Click to see the 172 entries | | | | |

## Sigma Overview

**AV Detection:**

Sigma detected: NanoCore

**E-Banking Fraud:**

Sigma detected: NanoCore

**System Summary:**

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

**Stealing of Sensitive Information:**

Sigma detected: NanoCore

**Remote Access Functionality:**

Sigma detected: NanoCore

## Jbx Signature Overview

Click to jump to signature section

**AV Detection:**

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

**Networking:**

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

**E-Banking Fraud:**

Yara detected Nanocore RAT

**Operating System Destruction:**

Protects its processes via BreakOnTermination flag

**System Summary:**

Malicious sample detected (through community Yara rule)

## Data Obfuscation:

.NET source code contains potential unpacker

## Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

## Boot Survival:

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)

## Malware Analysis System Evasion:

Yara detected AntiVM autoit script

## 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

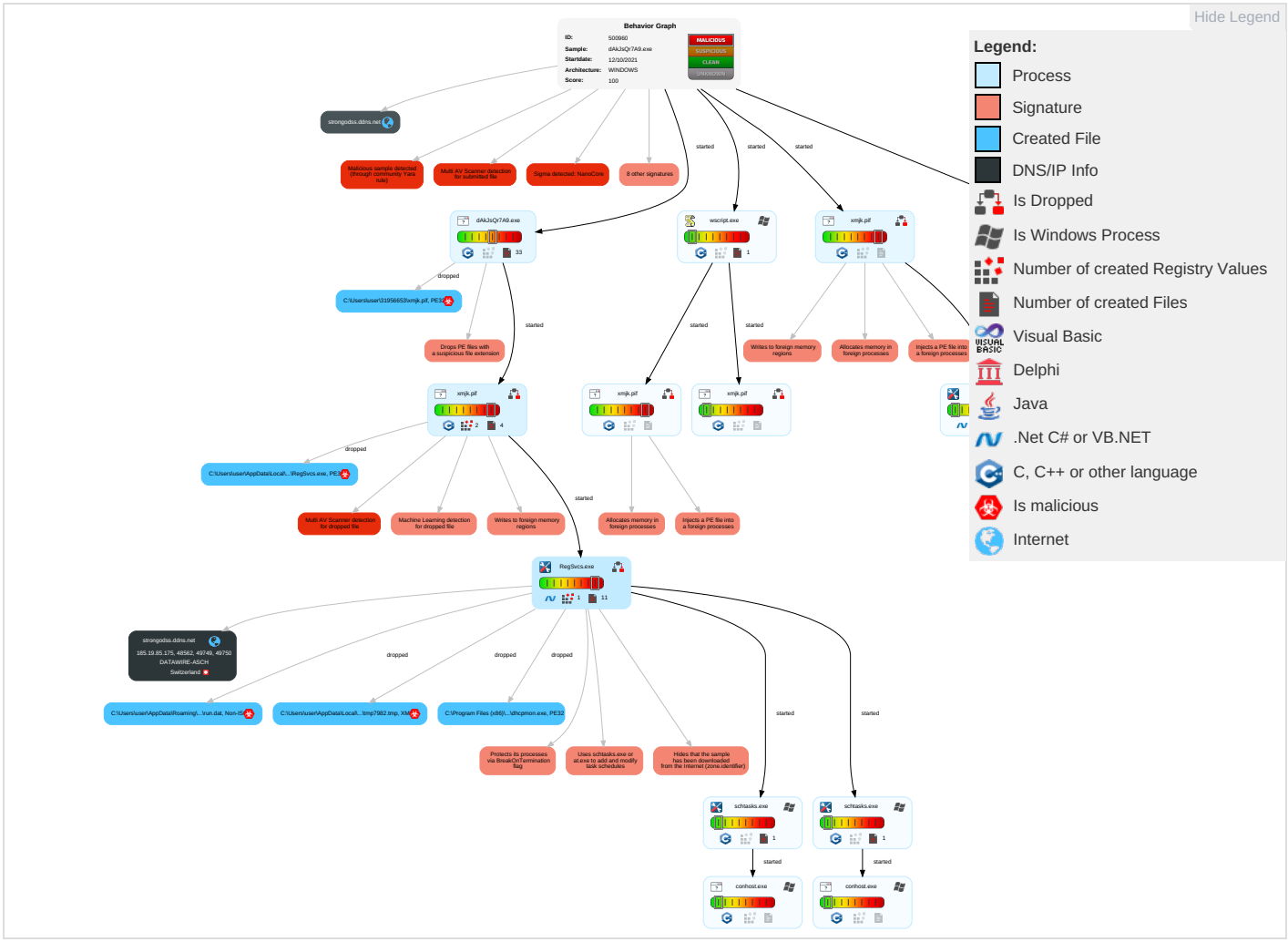
Yara detected Nanocore RAT

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Con and |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts 2 | Scripting 1 1 | DLL Side-Loading 1 | Exploitation for Privilege Escalation 1 | Disable or Modify Tools 1 1 | Input Capture 3 1 | System Time Discovery 2 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Ingr Trar |
| Default Accounts | Native API 1 | Valid Accounts 2 | DLL Side-Loading 1 | Deobfuscate/Decode Files or Information 1 1 | LSASS Memory | Account Discovery 1 | Remote Desktop Protocol | Input Capture 3 1 | Exfiltration Over Bluetooth | Encr Cha |
| Domain Accounts | Command and Scripting Interpreter 2 | Scheduled Task/Job 1 | Valid Accounts 2 | Scripting 1 1 | Security Account Manager | File and Directory Discovery 2 | SMB/Windows Admin Shares | Clipboard Data 2 | Automated Exfiltration | Non Port |
| Local Accounts | Scheduled Task/Job 1 | Logon Script (Mac) | Access Token Manipulation 2 1 | Obfuscated Files or Information 2 | NTDS | System Information Discovery 3 6 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Rem Acc Soft |
| Cloud Accounts | Cron | Network Logon Script | Process Injection 3 1 2 | Software Packing 1 2 | LSA Secrets | Security Software Discovery 1 2 1 | SSH | Keylogging | Data Transfer Size Limits | Non App Laye Prot |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Con and |
|---|---|---|---|---|---|---|---|---|---|---|
| Replication Through Removable Media | Launchd | Rc.common | Scheduled Task/Job 1 | DLL Side-Loading 1 | Cached Domain Credentials | Virtualization/Sandbox Evasion 2 1 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | App Lay Prot |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Masquerading 1 2 | DCSync | Process Discovery 2 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Con Use |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Valid Accounts 2 | Proc Filesystem | Application Window Discovery 1 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | App Lay |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | Virtualization/Sandbox Evasion 2 1 | /etc/passwd and /etc/shadow | System Owner/User Discovery 1 | Software Deployment Tools | Data Staged | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Prot |
| Supply Chain Compromise | AppleScript | At (Windows) | At (Windows) | Access Token Manipulation 2 1 | Network Sniffing | Remote System Discovery 1 | Taint Shared Content | Local Data Staging | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | File Prot |
| Compromise Software Dependencies and Development Tools | Windows Command Shell | Cron | Cron | Process Injection 3 1 2 | Input Capture | Permission Groups Discovery | Replication Through Removable Media | Remote Data Staging | Exfiltration Over Physical Medium | Mail |
| Compromise Software Supply Chain | Unix Shell | Launchd | Launchd | Hidden Files and Directories 1 | Keylogging | Local Groups | Component Object Model and Distributed COM | Screen Capture | Exfiltration over USB | DNS |

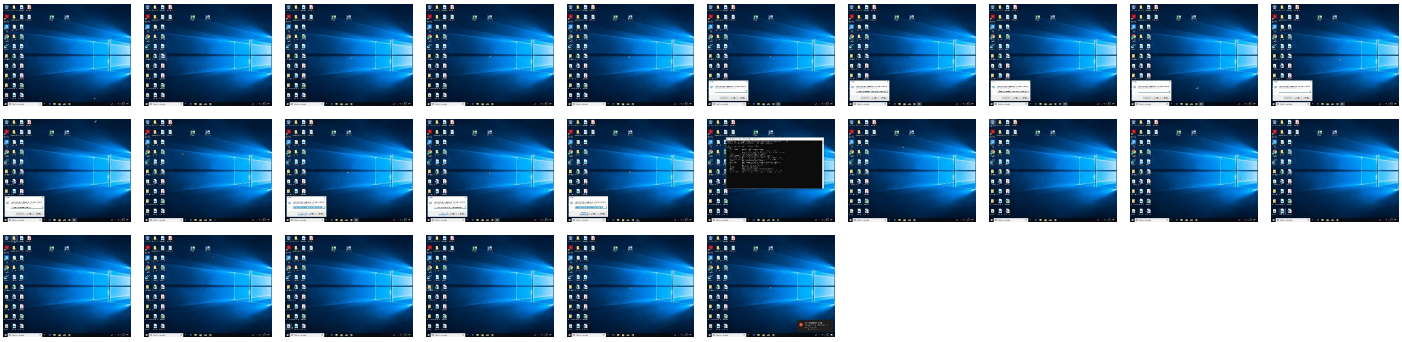
## Behavior Graph



# 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 |
|---|---|---|---|---|
| dAkJsQr7A9.exe | 59% | ReversingLabs | Win32.Trojan.Sabsik | |
| dAkJsQr7A9.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\31956653\xmjk.pif | 100% | Joe Sandbox ML | | |
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 0% | Metadefender | | Browse |
| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | 0% | ReversingLabs | | |
| C:\Users\user\31956653\xmjk.pif | 37% | Metadefender | | Browse |
| C:\Users\user\31956653\xmjk.pif | 56% | ReversingLabs | Win32.Packed.Generic | |
| C:\Users\user\AppData\Local\Temp\RegSvcs.exe | 0% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\RegSvcs.exe | 0% | ReversingLabs | | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 6.2.RegSvcs.exe.b00000.1.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |
| 6.2.RegSvcs.exe.60b0000.11.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 25.2.RegSvcs.exe.bc0000.1.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.onnodb.com/aetraymenuH( | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| windowsupdate.s.llnwi.net | 178.79.242.0 | true | false | | high |
| strongodss.ddns.net | 185.19.85.175 | true | false | | high |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.19.85.175 | strongodss.ddns.net | Switzerland | | 48971 | DATAWIRE-ASCH | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 500960 |
| Start date: | 12.10.2021 |
| Start time: | 12:33:05 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 15m 29s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | dAkJsQr7A9.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: | 45 |
| 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.evad.winEXE@27/41@10/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 12% (good quality ratio 11.4%)<br>• Quality average: 74.5%<br>• Quality standard deviation: 27.9% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 12:34:30 | Autostart | Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\31956653\xmjk.pif C:\Users\user\31956653\thjfdg.xcp |
| 12:34:37 | Task Scheduler | Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0) |
| 12:34:37 | API Interceptor | 803x Sleep call for process: RegSvcs.exe modified |
| 12:34:38 | Autostart | Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\31956653\Update.vbs |
| 12:34:39 | Task Scheduler | Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0) |
| 12:34:48 | Autostart | Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

## Created / dropped Files

| C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 45152 |
| Entropy (8bit): | 6.149629800481177 |
| Encrypted: | false |
| SSDEEP: | 768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC |
| MD5: | 2867A3817C9245F7CF518524DFD18F28 |
| SHA1: | D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC |
| SHA-256: | 43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50 |
| SHA-512: | 7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D<br>B42 |
| Malicious: | false |
| Antivirus: | • Antivirus: Metadefender, Detection: 0%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ..... ..H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]... |

| C:\Users\user\31956653\Update.vbs | |
|---|---|
| Process: | C:\Users\user\31956653\xmjk.pif |
| File Type: | ASCII text, with no line terminators |
| Category: | modified |
| Size (bytes): | 0 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:FER/n0eFH5OWXp5TcQfSOL0eWXp5TcQfRfH:FER/lFHIWXpDWeWXpD5fH |
| MD5: | 2C760FEAA61BDB817B1A1E47DB415464 |
| SHA1: | 4D4A10381CF79693E07DC12F6D3D2E817FE0F8E6 |
| SHA-256: | DEF99AF20BF09CBDCADBD5265CE8030CDE157CB717EE366B0D13CE979DAF87B9 |
| SHA-512: | 011F977A63C157775FF4114E6FC512DBDE71338F1C6F77CCEDCF916A5AFF0E0F4E1A861EE45C0C96E8FBFD01FA90805ADAD1AEC5A2DBB4E1D71F23F2AB16F<br>09 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | CreateObject("WScript.Shell").Run "C:\Users\user\31956653\xmjk.pif C:\Users\user\31956653\thjfdg.xcp" |

| C:\Users\user\31956653\ailgkjbn.log | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 566 |
| Entropy (8bit): | 5.474806202875037 |
| Encrypted: | false |
| SSDEEP: | 12:6RsfOzSb2eBfwqcTHw3I3QK5/ph6hoAen4PWh:1ZdqT/3Qe/Nniq |
| MD5: | 28E06D43C4A87B30ACF1E733562A4803 |
| SHA1: | 974D8AE0C0E74D013FADE83771E8115AF06E743C |
| SHA-256: | F2AD07A7279070982BF482DEAFF192A830CB9BB30D107D068BAD4DB614B480A4 |
| SHA-512: | EA06C6FA427D35E946DA94DB02D5465212DB2D9C28C1A233D435681561F57695CA95E849416A85A0993D7ED8C50FE4E1E3F43D24F6D79F273BA6DAEA8A00F71 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 00m2MoCZR08G6T6aTK9zimrgta33405Y9Kw39Ep1OTNB7x0sZha012w881321W35hR7lGJe145479P7256eg6m0d3WK3zvE473994B9alhKohV90i7..B70A879332d535<br>y2mY3h..YDc71Y83x3km48rSYe8528w9N637v97AQmoa9382X7TT5sBJ7x23u9KhDnv79oA82nz0Lu8W96x5QZ73d0s8..h08pB6JGffFk3eVwuJ13R13Q7nJM96LRbj3V<br>5PpuClC5578K64OSl695WAX87dw02lXaShcd475MA2izFFNr7lCh2sHm4a751o0u740Na92322h2eH7Jm1Y692488653kGY04G5Y27YCH19035..878u6UFRAm6B4rle1N<br>GX3340691R1YV9Wu45S81Ke4371470583153Li6n588M8v9m476n2881uW4E14d697V1bebB128lkR4c6E4v1KM8NO2UII9691XZ2wuP0Ziefit7kZJb495OZ88Z3525vv<br>K00Qiw6WRGJ23C45s16WP281D7Nd985cPn2926Nw8hn4.. |

| C:\Users\user\31956653\bwhgjbnh.log | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |

| C:\Users\user\31956653\bwhgjbnh.log | |
|---|---|
| Category: | dropped |
| Size (bytes): | 618 |
| Entropy (8bit): | 5.492211285373292 |
| Encrypted: | false |
| SSDEEP: | 12:g5mQnoBIIzM4IsfkXZlqgjwooNtMR5i1ISn1URtd42B66F2a:HQoBDhMPvjwokiR5i1IQeRD42B6a/ |
| MD5: | AB4AB7821096064493E76399254C86E9 |
| SHA1: | BFCD02463B2461C33E42D20893E25E3C11FE793F |
| SHA-256: | 20349787AC0F07ED5749CF5676CEE6D4977B714A4716BB1B3398C04DDE439B9A |
| SHA-512: | C83E64D7262E7CE7494CF9EBD89D6F04162B59C39ABCC337E365E3C7BAFE6135610BA83B8084F79159A2D107657697B366F1A286F77B9583EC5742F47D1B2E81 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 94uuK2N6xOp15273v15vm9i88EN6X003T230V44dYb9L167XVW61a9ege0iu4VSk8un8l7kKa56Xen5t0Jq0uPk1S6f11G054i7YxXV0u4WPTKJV2fO400W88o7853let9 ux8fqN4J0wq07OEh71H..JB99588393H4jOVQVz..3y50Mt07033210..2T582U0WPoz4d0dX7327y..Y79nY9jL..niZQ71tjipa0NZH9Qu8738g1l75bz034vIzFW1371z6J6iVu31 qqXd8K06TT9aI22s5a..VvMa84ZuW5RoH6mi80Db844T7Q35fXyq143grbpCxy2M8N3G14WJ67J0nTZ89151433VWi9q43Th09GDKln3TsH7Z818e0a515299a6UkbtgVM 2a15..p2SG4W60HW6Q0u9703D..d5py1IYbx7o4s3G0kQIN5EDs18327M0F1R37798d85pJg698I6gH358kpL14W8p1U7ut9d055xqq40k4W59M4M8xxuJp1H78Dxm7x3R 55tDD987VNswG9BTT96PDd0t6W6409V56w53gooD73o1Sl72FP4M03p6O39ND0842s82TM8G86B624C5NR0637.. |

| C:\Users\user\31956653\cmeaaw.icm | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 502 |
| Entropy (8bit): | 5.518570874996825 |
| Encrypted: | false |
| SSDEEP: | 12:GORcQkX9ftOfhDkKVXWyw7R4GRg4UgUp5yiejVm:GO6QkX9f8vhWy4RKTDFejs |
| MD5: | 3499E273898AD561A098D9FA4EBF4F99 |
| SHA1: | 94908C6032CA83B4D9C8155B90F476A8CE217F9B |
| SHA-256: | 16612DA64414084D50A38DDB0B48ED8B805914655FF0AD67775999E5052FDBF9 |
| SHA-512: | FE676D37932C7E12751CEC9D7A580FD9A78D94CDBD7337F3F5D397E1549E7001D9F86EC2C0C2437CF63BAC2DE81CE23C3EB5B8E9FCD4EB93F4121A00419F5A 91 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | OT8tbOkcKZoy0L9yuH835M6l99A99s6qr2LI..hb5xybiUR3s8z9HdN09D7amkn8wk1fn2t68w707YF43U945LE58A9s1KLT59rX422T4mP17h97Fx85z9h7U5v5GJsHPb h5g7Xg04wU3860rLJ764noN2tMc27H..5goUt203326..hOiB46168b108uC593260Gt085J14CY7xe0Lc8F5Q26H25U5i34WL157g..V8l98891YD0H5rO989mXsd4o4f 09L1565i4WNCf2CYTwelf071j5a4Vg80nxvfk67r3N5S1y1307ZNi9JVTnf07C..HB097q341731O8e70rfVz0cb8dy6SMyn0PDKqh2ER2K9vN4h15764w2K005C261..3 59H42b675Tm5h1NY0x6o9y0ON9Sot151pBkxmM4gPhx4t85mLBykB8tSx4f5k1v2293387sToKd40G8Tf35b5fo670Z3zJ52431966pp0Tc322.. |

| C:\Users\user\31956653\eblsq.ppt | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 49345 |
| Entropy (8bit): | 5.587895640570609 |
| Encrypted: | false |
| SSDEEP: | 1536:OZ7+4wnkTPomimumHx/io+9h8ALSQX4StbCyh3ZwRF+Kfslj:SykTgEumHxx+9+cSQo3yhGP90lj |
| MD5: | E9F03E752D086599C5F285B4CEFE1F52 |
| SHA1: | 538098DEA70D96CFD1A070A8D8EB824D7CC80DF6 |
| SHA-256: | D65205429A1F0FD8FD3DA688F1C703944F41128D543801CFF8E5E7EF3B11448E |
| SHA-512: | 0474865940482F84D25C94B3F6DDCA33DCE370932E03E06F45C46AF25BCFC12770B8FAF6C116D637C780E04D9A897084A52FDBECDBAF78D6C3A7C2C9162C3A 2 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 45nn..48lTe3557k9Ln35ft0Q9d7c9rdO4n7N8929yK2h8E83OK55K9..OG3b553TG5UJp7BNj215F2s70B420oHRmb6X870Hqe..M0L1TUZJs068FD43aX431Bx160e7N JE88jh4H7X0Y866..cS40557uvPo4O096h5Pi2r2SzC6R80nw35M4Dm6gxM76770..Of2w827l0T11Nos280657E9Ye5JtWI00Y00q5AXN24H7CVeR1l6cg..c7LQHKmEG 226TMm0G199BMG6IA43WVmGzq2B519U2npz6CeVu06y9..43o6Io318396l91322MR0J6v2l6w409n73143Qb197tRP9..9wUvKa079025dHY9Lef89Rgk4l19Lp34h171 KjC5qF..1q90l3563j8j5D2406U5qbApc0Nnc3547qoT23su54rEJ1s6h5eQ77r69tU5B2617..5C82phDQ6F89p67w60y0q14P442xZ2222V74de9T8O46450TRTR8M0T LWz4..633M4J5092iK5S1vcW4DWyAWJ5497VznKN51465l085lx37ifg00R9JfXu6YgDMGS990WxmGANiZa71GXCK..TsZ64hIe514956706o88Ac3Y3Lk2Z0..586fr41 3u5n2WtjWvQ39J938sTY4pMHV316v2mo728DXENQ891raJZX..Uk32qPe4rTR11T84or7N1Ou72i15C82Qx09EY61690bZ2XH93..v699028vg3o2Z2kombF73210k8XAd P42Q4YL66177x59c0U64w9jUd41q9kRtC765..t7lW0R6Ws4C8o1qLO1609OiP764WH6842c7F1R7Kv97389410iBVp807P2MH594q431os2oU5VVp7743..41O94B75G9 987171Ny31Va935n2rR95rx4..rvV6iKX3oa3m1263y40IOK6tXUi2P45e8X05u517161dPE982waUQY4qTiX0D12o |

| C:\Users\user\31956653\ecbgd.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 502 |
| Entropy (8bit): | 5.492718450958176 |

| C:\Users\user\31956653\ecbgd.exe | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 12:aGRVZUPx1L2S07WsolsYAEnvQzcxyeDYmt2GkDWDhla4L:1VI1LNGW19vQzcxyKYmsfWdlaK |
| MD5: | 28D423CEA277EC2F8B385968A741F27E |
| SHA1: | 8FEE5ADF02336520DE0E71FFA55FBB80078B7048 |
| SHA-256: | 37C0981080756F4E532ABCF3C64B87F27C62B2C0111C567E2183652DCD7852AD |
| SHA-512: | 0D8BF1DDE5C9184F98AAC8429D819ACBE014FBF42BD7D4B1F70B8E10CBF26AF843D2E88E78713AD324540FF7993838CD07FDA262FA60A6243C071013F9E82B(D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | cwQDdR28tR2U7x276CqI11XC7qz5487Zs86160N60P9Y3T..94P49acTM5858idNIdLUX101o4T04395w2x2jn6Dnz445Vu69WV3xrZ1auBkFA6iEI097Aj7He95T38SkMkx92BZFnN722484B3vCWA8IU50D08mvO86s6oNay52u9..SQd2J08X869CZ81pz160P870KA792p26PyM36A8K8jT8BASDAL4jT6z8a2p427z6IMxWb00Z2lui6Ko9fjh5r9a130zoxn63L3H..x8SAm12v6DT50192n3k72vVFUL0X9C0F388..5h8H912673WAr7949D488lL6rMYC40460ai3sBiL815E11d5L74McnBCgH156n0P7e1m103556D0rX877q6S6G2D9Z79..UyL4r8U0xOF92O4i3Wj9310279R5UC103p1t1o252166l52mpcwgegLR86ytr543p1y7j465w191bZ3TdGD79498947w.. |

| C:\Users\user\31956653\emngwc.ico | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 586 |
| Entropy (8bit): | 5.5426308661865695 |
| Encrypted: | false |
| SSDEEP: | 12:cQjeQ63r6OHW2hE8CPOVCaIGVBdVXe2xlPSCkxODf7T90Nsm+Un:cWP6362htmGCZGv/734Ob7pOH+U |
| MD5: | 6CD6F7DB6C60AF4E1E524759D71E579B |
| SHA1: | A590D0F3C84ABDDACCA95C3842D5BAAA28C38844 |
| SHA-256: | 88F39B3996B987B2EE399EF315E02757A357205EC1CD34646ADC8B6E940A9B6A |
| SHA-512: | 6091C410E324EEF9F02079CE2AE8EA904E74C824FB8BDE65B63DC4F1F56D5E67C491DDFCAA7BC0C422AC5253A49BD909F10AD4BD8D9B655390D4CCAF9DF7(4FF |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 5l34999V1U701578UiY687u07758QM8nX5h07d4iJl8d9Q3X3070u2L31G82NDs6d02Pz5d5869qgu2DE213a2277540T41296B74h47l5z..y2qt7g86a76wiVEb03NG83U92v128O0hy2aZZsKUw46N2tfQq8mNt4P4063nyH9vM18vk29TYA4pO4OJJ0bjPNF2pvCm5gO7..u8p52zx9z..p4l49sP879..b00078os496c064P6xyB38..F08490JFy0gjVo474ghm88Edm5qe8nDcoK7xy3QaLmZ21677m430Ny..0pNiQ0086N77Z4l0uO7WZE2740kfZ4M4idL59yb42245141Jovz85Nv0Ah1OmU2t78m1zK3B9G9p276i61NqwYvw8e5412BUl6X0d33J2QEv37KC479u98ZbHB8IT2YJbw889iiq4Q51f6Wk8568x2jhd4l41..Ty0gNrYJR593301k8b7QEa307wBo19Z5qy2d3ZV637rW64W12Xkqs0u25fFGE8sCr225n7rYX9rH5S64EeryjmA1eOmsUa00s6aYofVC9ZNY1mqXKJ9.. |

| C:\Users\user\31956653\eoltp.msc | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 528 |
| Entropy (8bit): | 5.493405913038473 |
| Encrypted: | false |
| SSDEEP: | 12:RiGRHEwjRks6woDA8CmOhFQWAv7+++B537Vt4w0QZ6V6o4:Mxyks6FkRm6qPza7H4wV+6J |
| MD5: | A307ED59D7093C9D83D305E38E48BB7F |
| SHA1: | 82DEE4639CD41DA817E1434C276B700F84310592 |
| SHA-256: | B31F2D309D1FCF67725328892919420F08F51C7ED41A8A7CC238075DED84E5AA |
| SHA-512: | 57E8AE3E60B843864909222F45865829F44825A257152B4BE1D0DC2EAD73F6047855234BB4E373D868EFB0494F7BE133A651FAD0648D4E3B1F4215196F54FD7D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 4arTEvaA0230Z9722QYxJR0996E3c3rck7YDP68p6H2Cl2H25po2C0Z63cyEkJ9P4V1MV1WisAJD85JGn3Q35k8K03150e4V2tLri052drgx5eI5v21J3113A..7r6E52ioaZ2Vnf42..h6W009K454h6T2ac232We6SkLl909lYCx4407092nGd2P47A0fR01ge201PSI5ip8J3v3Fj9881znu23s71cwI2O7xH71179jtQ47Dwy9m4..80ZKX7B85nfs8EwpF5z9NZx2i46T6l5T5ey00iD8YON87m0411m91PI55IW19eu5J16..s8l29521PqovEd37d8..6Zic383j9S2hf4ka92bhVhB8W956E24RF80vC0I66Q4807DjM0oOD1QHh10C0B6V5O18K6JT3Op9G0n23b7218471GJ7G6G6R394..7u643o95m6Rp00pt388r668j9l395XA2V54jV12160Vp78Hi40ae40C2eDg1Wr42O0u8iec76hPufB0s92V0L.. |

| C:\Users\user\31956653\jdmhhwxx.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 518 |
| Entropy (8bit): | 5.489925874272235 |
| Encrypted: | false |
| SSDEEP: | 6:2FRNmMwFTAZcnnG5ahpG7AGwtWF1Ccyh+14qMzT49wpT0SAvDNpYHJ3N9HNSXpxH:ybmRAiLhxtMA+WzTrhwgJ3NmXpA1V91q |
| MD5: | 1917FEE95C8AF5BC4CBA1345D67F8A18 |
| SHA1: | 7DD6E4E5B44B032C93B0911DB1328A70EAC80DD7 |
| SHA-256: | AB0091F4F773536CA9D51BECA3E5AD58ABF2180AD06DD646C7845D1FE53C9A11 |

| C:\Users\user\31956653\jdmhhwxx.dll | |
|---|---|
| SHA-512: | 7D44BA47292F6F7DD84F9D8F74F2C44FB7CF09628E511E2A18053C9B77AECFE85BB6FD16AAB1300440199876A3F5D093D2AECFD3E3235B26D822F6D195039D0 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 3v54eAI0Q966MUq27RQ32z6336P6Nc02gZuljwD2ulp34p15w84e811p9q3cFW5CLe3Pf2T263967m535N5f15Hu616G49Y6Nmcsl1lqEYU744ca1po0wBs46ax8boeWx193i3cb94k494UU..aQUG5eUJ00..qy4uldg7zx09Df0426p8a2G97022588U92741yru7318W5foEB81785vQ04872M..o5mh3526hd7rT9y3X894rL5..M48lu8Bc7on3kh9O833fM77yM0iq900R0zBrpfF4ng5..md78V187M90M0Y57Xhnrx8O6dd9088o1r5piV2H1755p2E4k..c1N4U58FLvbt71..0d1IYA8u091P3675X0G01GcJdi92iRc4A0955AY6n6x5oK94x1lAb9s08pm1K2U7239s..n2hIM91rbxJ2lHw012X6pCBeUu7v806T4385x3818Ji2urzM4jS50q10088DoU0i25XYv15Tu5x0Z9I51d9Et25.. |

| C:\Users\user\31956653\jhuu.xvs | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with very long lines, with no line terminators |
| Category: | dropped |
| Size (bytes): | 430098 |
| Entropy (8bit): | 4.000009436079219 |
| Encrypted: | false |
| SSDEEP: | 6144:y/vX4WkRrUZQvMXfnVxAmsVlcUP5sNqiUD5sGZRtSH9:y/rXfVxAms7P5sNqHxRts9 |
| MD5: | 9990C4B0B0D9FD51DEBD402EB04FDC42 |
| SHA1: | 8C1CF56BC1F2A715B4333F6BE0DAF0BD9E61232D |
| SHA-256: | 08232B8E0E07D352C6528E64F6CDB7EC7D52B1066186C64B24E991F731F55FD1 |
| SHA-512: | B9C7C3678A05D5C30609FC2E4663D34AD3486D4FF587A517B4BBEC8E6B09DAB47B93F1C2EE3117E7F15F8FFEB4BD6EBA08EAACA89576633D65F1ED709710854A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | A323CC10D6D45EBA804D04412198A8F1CA4FF2816777492DEDA5CA833EBC6BEB1652C8B2D7257FF7AFE3F9E7D5E1398D725CCF0187C11C78E156667265EA81F4EE8C3346415608FD6A3DBD003E9FAF958175C77FA22E301B8BDC54F28084F190C3B3465C12D1C4C8C45392CA69614C2D775A065B977EAD6831786C39921F48DB5D32576ECFCDAA8C11C8B3E5F572597E18DC88656ABF9FD95251FB82FA57DFF297920B69DF7B71C922099F85AB5D48E38DF8972E58CD812CA042C015A513DC449E316F52627CB478C5FFEA8D1C11527718122B15BDEF346C32B06D0BF9736393F3922FA4B2B970EFB32FC46C15AD2B93F965F73C56485238AC222449F7407283B25F75016C434D731C98F841C3C0A006223F2AA959AB2D507BC33328632152EAB227C0F9072D3D35687219EA6A22DBAEEF7F8C4E927114D13618917BB62393ADF2869B7F766CDC7B395CF94A98105010A696823C6ABA93BEBF69259CF09C0EAE7B7FD4DA374428124822FE357BC28579AC3FF3141218AA70E5FCB20B65A59A2EC94C338E9D34E38E26D2F55C723066238C17068B9D1433752C0714CA1F1014CDBA7D5B6DB18410D66654465285BC38D1B7EA402AE50F2C0844760882CD9B0FD455733D82C6C059D249F81ED6AC1138D89FDC6B1A8DD74B19761A7D22E179EA4D63030181227DB4EA8641FC8CEFF2839EA3A85CDD |

| C:\Users\user\31956653\lsrlf.xl | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 610 |
| Entropy (8bit): | 5.534043765719752 |
| Encrypted: | false |
| SSDEEP: | 12:oBXsRS13pvqiTWBRRYVLAfTNuGIEwkLSXQ2rIQfwvVWQMZ+xkWE43+87tzSH:edpyIWzNbNuGIAL+f4vg8aWE4u87tzSH |
| MD5: | 7F921B7F69F739F05907104392B9B518 |
| SHA1: | BF6F23AD7E768EA57B1E686C80C296258E8EE4E0 |
| SHA-256: | 3D631AF450E4C57D40CDBA273F2670B1CAC8C92201423FC022303922672D445E |
| SHA-512: | D723F53A420E95EF46835022FB6C82359BCCE6E54E9505434CB7D9ACC4A02DA30DCB6067E4F9546273143D18611085D3B0EC931F742C57FC78F9A077B05366E2 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | P9g3B7J0EQ8A0613MM034RZ..M9V57mnig1L4HLu40Fp780L13th05oOFoPa1yx0a03iC53472K7r6386rh266b46XU8Up01c439UIx9nTOC3T56P84602BX2Xm65Z..9873zd18Ps14ei2D5hyKOim51..63YJ8gUX6Nts66099C81wl85GNK192K5XcB7C55h860P7y7i53t1zw9Z5A7G528ul1d6P6m..K311G59LR420k4BUkC3zjSK2PoWWAbQ3zbN1NW2425UGt7O7eC4y13E4k8X0q484xB61A1044541d3el5HIjk5f..5U0qr7LW0Eh1I40YO17Rg1bFb1eSeUt2..61SkSZ5ru6293RRE75x04466o0Q76aR5d992242rh5XRi4mAc204b9908f5Ukr7t9P4Y62762MS0TPGh2ZIlaorg2G00jb8a5uXRT0L95Oh3h1HF5X4LLv429N..40mWJ9twP6S6Ee3c75PEk5pY91Wnlct8909I82Zzo7Q7gb4yD43Q60875Q6X43z36H8Oi4RA2510mUt7vG731GN45aR46e1VHm1rtq5059Y72kj44az29M1FzxPH9HH63r53c.. |

| C:\Users\user\31956653\nfnfdq.bmp | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 571 |
| Entropy (8bit): | 5.4258865359256285 |
| Encrypted: | false |
| SSDEEP: | 12:WA5I86YrEEaJiAiFxRr8bGAtidb8Wd4DqBxZxSKVsFxF6RkO7s4:WSI8phaJiAGWwbY8kO7s4 |
| MD5: | 4D5D0D4C703103475DAE81F0621B8115 |
| SHA1: | 38DFAE875765BBEBD7047ED770B8346EB9A18D12 |
| SHA-256: | 4B8F7FCA38E042BE1CAA4289B8CEB85579274EB8989BA5F1E63DE9315C8DDAEC |
| SHA-512: | 982DACDFBA4C9C316860B04DD9C53D109083ACAE63CBBF4B4B20E0F6B8BBCA3551B39DA1D0855DE6DDCA895CCAC19209EFBDA31E9C9A0E381E0E7E672C15C20B |
| Malicious: | false |

| C:\Users\user\31956653\nfnfdq.bmp | |
|---|---|
| Reputation: | unknown |
| Preview: | w31uU04605p080wWn9L574Qxrt8M4v4a0Re50b48YiL0171ZMmX211Y3i358BJX9bPW170968Ip4E6770kEg99Zp0jDKm5B6..5Iucn9y5..36Nac54031f3h..07Liu2043h53Y20t5JCY1QK93l..73W757ON5090d91351mb65EM5J4B098q468PDDm4B2mSW261vQ8v4x18O5MRW04W4I8ILn12g1P69GLf492y4In12OI4Q38m4XA04D8kk82t3Wi5R6m23coO8b1Ab9Fi70P885d43p0g606Fk905P3845sI8..e8jL2X2010k8D1K971oW550BUfnY827F683g9E0DSC75sm23u04ydW3S6Dm389vc27643X21TS96131..171TBRKP75Z16nvt6A2EJw7wME5TRf3lw6I63ptQ419N255C5h7GFjr2Y2lUb8X3aOH07n7kN186K0n6103ESZTZ..IrQ5S7YB7MJ1s6b8012jDCD5l79784s6P0MM39p87fb4Wgb3tP8v08n6xmnLpG8cq432e5sY72555187mJ95811nl.. |

| C:\Users\user\31956653\pgbpe.xl | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 551 |
| Entropy (8bit): | 5.521649808206063 |
| Encrypted: | false |
| SSDEEP: | 12:wHB8ipEd9NyrqH623PyBP5H9T4k1T7EfW2bNXOw:qaipEdarayh5H90k1vEfW2bFd |
| MD5: | 59CF11E97D4E3DBB74BAA742880DC604 |
| SHA1: | 6F488C6018EA5C6EC1F1D13C1F4590DBD71C3ECA |
| SHA-256: | C2C2CC14FC87666E687F1AD205A3BB967CE97BAA15FD897E1B9B2BFCBD7C3F79 |
| SHA-512: | 3BC00980B36308785A63DCF809DE2AF16AC48C2FAE5C6CF3AA170F3AE896BFEC140E704D46080BA40A3739EAA0C23BE96B684451CA912EC6852657851886DFAF |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 86oM9Y905KqL541383gP0F1oa62Bj5W51Fc2zkc75nd2p2hy0h6NqGS7K0oh61N..S0tFY4a7qmq884De0fJR4F8lt8963cK4xN7x0891F4yl3l1Up474dmC7ksC94w685069292990O4H8NY8Z5Eiz6S55E204q0jc0L..81Z8984Y4pO82CcGc44Qp2P8K1v6N4FcMj1TP471CQj7qSPDZ675Q322N26S8m1dQ5848M1N501D2W6bkv9V9h3i63ZgBq7ALfP7LC3i85pSJDaGgiWWg1R2707b38V4F0z40Pe6XY0FiIK8..8zk7Ai86x6n23l07gZA08X5..1B602O2w46xEi4B4..0Vb15290g65axuZH1RQ81y005106r24Ak972514576q689K12M578589m74701g6CafFcUjcU5xji..P339m92637O2IWsr9eQSmU201Cc0es4G..qfyfEVR..gi83sd8McL1i30L8dajps74O31eI3X9oxC7s81U97vQh2PWg24A0M64Y39AIug21U8tO26y.. |

| C:\Users\user\31956653\qixdqtxae.log | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 526 |
| Entropy (8bit): | 5.480927918891487 |
| Encrypted: | false |
| SSDEEP: | 12:LQFtsoKyX/+Y3+oddh2qZthuzwAouctvX7vB2RcEMk:Lqtl7GrQd/hgwlbPS1Mk |
| MD5: | 1867000A68FB9CA6F42E190806A8EFE6 |
| SHA1: | 48D57FD28D9E440D165A4D7FF96C362E5899530C |
| SHA-256: | B1B7796D138B12A9E3CFC5BAEAA8A136E7B09F1EE46321686E21EC917F9A0C4F |
| SHA-512: | 6213222C7633201EAD0A966811AA7C6645082880B5EDB0D1D618EC10D7544319C64A1DD2186B5B45BD5CFA5498B702DF13BD52C3EC26EA574C01B669068EC1F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 41T630V59608190R9w07C8b1w54sTX76B455rI081902o43l11y5Ry0qr05Z79e7si3g0YbGX3P6r4x5o2LF7kt8Wh9l1T420J7R2PfV39dyDu895J8lQ706w3g55Wl..xl6pUoi699S8lik6gA7n6A43qM9Ak9WF7bZY6j919v3..957dBLd32lb9z9960Az947MT29e24KgRURO865ctsf5I54X69mZS949GG752H5..513354VO70cRZ2N0LX89F413qEY5JZn21578B48fh4moONq1h55O17r587eho066X46y9G743d7U2g74lD4a218eL89N8SIbr798450SEJ8P7F6H5..T3Fm9ro385J5vxv3uK7VK14p2nfoVvII4u64u4cy6443gw4i60e583ORXOwI4v3jMA13bV9y7Lng48m03gdl3h9607OR57y24..60854dcN1C39dE719cX1El97RCI15lQ09570fKF4DBGd9sza6MHaH8lL0ar63L3vL4R7o9yF.. |

| C:\Users\user\31956653\qsfuelnwxb.jpg | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 603 |
| Entropy (8bit): | 5.461083340782776 |
| Encrypted: | false |
| SSDEEP: | 12:Y+cdtO/mSL6Vs86dZ6vySV9y5CaQloNHXj5KDoI7BW7p:idt/N6/hmCCaQlSdKDomUp |
| MD5: | 0A5C2FC9ECB89593B6B68AC91D90649E |
| SHA1: | 7EE3267AA965D17A80B4B20B68454C4077FD5AFF |
| SHA-256: | 55B1A7C4E9FE5B08C145BAEA8FA172CE4BF3EC86A4EDA385E73A72B02E497D47 |
| SHA-512: | 6144231D8306BEF01C2BA6D647D44CF7185B4231DF34A24105B6A189FBF0ABC0F3BA7492AC2F2DDDC5381670A13BDB05B0C8B7A1557804492D9000210D7CE82 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\31956653\qsfuelnwxb.jpg | |
|---|---|
| Preview: | MgCIGBPQ92xe5Kc27us56j05e3Do38a22TLFwj083b020m2K29828Kv25bZOY4611D8668ME07otc57iXLM2F39H8g2cD91rj86PjD8tK0gW6u86WM070C6L88..8g83X0<br>a298l7NbPy1d8yz9mpQby4kh62T4Z180T6V4t4B9113631mMS3UU2x0rjw0u5NzblD0M3X5z..q5qQ7..5YqyVxs37Mq1984Ss49R859yTY3i77K750rde3vh001GDe4df<br>E2d9i68Zf6J0lr001ZYWAr31z6z011h09w22V1Q22M286dLLi5z2yEljM9Wl2c786ux..06h34F7h0iE7PTD6og8a6s51430g660tc7T1O7p5E6T2t82T2Q80Z01a55Q14<br>mCie9Upq0E62Q9d85C2510QMilmg39PIT29Dfj08cp2691wDi39esHrCOB889ZQ56jm2v19ke520SoBcV10b1..14N9q44149ntGM..70fjg5M5G8j5TE5b46W8YmH3424<br>1Wb9cVu01664Bx3N6e35588946t79N8h9Xy60836XM1w9Tw3cz88503W39Wc6TAg95925B8q9o187483F.. |

| C:\Users\user\31956653\rnudekk.ico | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 524 |
| Entropy (8bit): | 5.486830582958616 |
| Encrypted: | false |
| SSDEEP: | 12:X+DA3rd8COUO+zUHzqFiKj5nGlVmTfvG0cbIx3R7OFJRBx1BVGoGjep:u03ZZ7O+zUOFh9ngVmTXG0cbIdRqbp1T |
| MD5: | 6E04A18D33AA0C86F8B718DFC6B2077F |
| SHA1: | 1794F45151C61ACB13E54D0F84C9815FF9572E1A |
| SHA-256: | 605DCE07B7E1986CECE7451A82684F1558617D896CE4727DD7DC0DD7774935F3 |
| SHA-512: | A9376B51B80C576000F25C8189F46021E8350A182E58D8C6CAD972937C059D31516E8D59138C318219A3F5BD9E5F1223F2DD0B9F1340DEBD65AEB22A9F6D8381 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | H4479vi580882Z812v882E86q3VG56z2m393jMVJeibL53y02OCY..612z6Lg0k19pKgr3jQBR8i774v96jv1955zQQ5D7o43v68yoN3kYkE4723c06lp4A804Bviqs1Q8<br>87X67R2ArisN76d6PY61EE014bl1L4OnlK0915263HU7Y777m6sv6..c1j0e8YMj450Xxi3834gtmAGZR88872cz9D4Y087W2e66630j4a..RpYN3onxEh8t3165I6E3zi<br>I5V5R8HH5427PaHe1hpI2jw44l4ju05ym99o5k9502j6L82pz70ST88u24N46JITW4HwQ18nIat1s9p8..6Ax4lD0F70mw8g0K9pnh9Id8A7jl9cTS618BlgL0B5ZEQ576<br>L44695B9o79Qw5e2L0g0QL8h27w374qv9D38Z56SU0Y0bS..81JFjB16H717W9qj0QU811765A0v4Dj36jrq43WY746I6Dh10szGesQ5F46V1AiN874JYuy71aez6aoCPixi.. |

| C:\Users\user\31956653\rpxeq.txt | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 520 |
| Entropy (8bit): | 5.481999414152157 |
| Encrypted: | false |
| SSDEEP: | 12:SjnPOsSS2ahe8kdz3kvGKxskGQlt0j64/keiXGWRyq8pefUIN2Yy:Sjnmsh2qe8CjkPskGQltQH/fiXGWRyqY |
| MD5: | A900C8F319EEF4A0E676999F344C5D4F |
| SHA1: | 9AA841963FF4B3DC10F8744AD184BDA11AD52B10 |
| SHA-256: | 8234EC2FD54B7979672FBB55E012C97E9B53E26D7CC641995C903CBEEEE0F07F |
| SHA-512: | C5D314CEA5C138C3214FC13E73E0FA194CACA8E2EA3C0F780D190B7219242D3780CD3D9E4E290EA68333317C013F3F1DA92B398EA582F9F69BF348E094ECB95<br>E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | HVg2s6Al0xkx00Hi6I1EA8M69oVX3uT66R27KB0N113W8U2N1Zr483ib8R7l4418QpUw2v1467y4e4EFtG..Y0T99h4o62b37ue6S2HslPD6f35941e5323Q48b43e5H41<br>4lxys4b9N2Z259V2hy6X44S7a1062hQO0Y0x16nY1Y61A0MHZuSz..SE0N6Q2N2Aly2seOPCX73D1c0W6Q043m7v2Xx79f0h1Bg913x1Oo4775576N35tA8590yT2Oy98B<br>qo603q1889f0666qe03X736TF31m9pyGi7..5zFh7917ldjl41562S6f9s7Z9..mN1m7R103b15u328pr3vnri1MCX3A28595cwGdu18K6..Z0k52kKeKdnb8CB1N4TMV3<br>89j63C1ka34957Y..150X624..2A6q3u7725i0QASjb0i65r6Q2227G861v00WKtzqzC79AfG1i89vE97mBL2u8F8X6z2z0ItZdM1F71X9huclz86bBy28lB5jv1009R.. |

| C:\Users\user\31956653\srveorm.cpl | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 529 |
| Entropy (8bit): | 5.443698259483672 |
| Encrypted: | false |
| SSDEEP: | 12:TGS1W5yztPSxuyOqhx35J0ZOPAhQ/TPaEHGKWfHz87:iwPkPX35JcYTCEjWfHzM |
| MD5: | 2561FBA5E942F77FCCC08BB6ED4D7951 |
| SHA1: | 9EF612A45DCC959BED9B4C1A065D96BF92FB0255 |
| SHA-256: | 6E06F3178B983D6AEA07C03A01AE8433296D6A6D1C8FE0BCA1FF881C5A5EADC4 |
| SHA-512: | 8EE80F7D9F2BD4B4ED0AE29789D6BB5A7F4BA85A0699353A735FE46024CC99DFF9F8BE3D3CEBB8B4DCD41C1D94AF46967D65AF870799CFC11BDDA62E2213088 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | Hp7d711F23724sDo2T1wpbg3..4nzR3884P303h7l672153R5B1y83k4Tn10..XQ598Sf1x7M7780JiC72KU7Q28s20V9k2f..265l64y689cu8o3D01L4d7FVv9O83v3A<br>4563924rv7T21J1718UYLM3nQT1w57rh9rVig293pJv975t89uDF3v4T7549L5q1Xk517fnaa89y7X6..3x82t7v5umXW8sw788qx1y40OQG4T537Y09V2Yc4QO8188f79<br>P9l30Ibw0r8j6D8W0A08Hdf3509qHX235wxB3Z4WDw57748SY98636fr1Js4I2G6R..c97X53Em94214gOj06m3k456QufQ3r1GYAI10sn60qj0o55698Nys9wu6532R9o<br>eLqD3ad54k8w03Tch0814LlIV6v5L6G329j6X7025g55m36f79..7z043KZ93h3v6IKW09u8FpTJt271S43V7u0G02p7i5n8y7Apy0NnD0DDj1PB40NMtWYNf6323JTk35<br>T31PJke.. |

| C:\Users\user\31956653\tahpojnovs.ppt | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 517 |
| Entropy (8bit): | 5.4730474782292795 |
| Encrypted: | false |
| SSDEEP: | 12:mZUdKYYOy2QpQ2KPgd7v4c6fcJ5WFBJfdyhdAm:mGZQC2eiB64gt9m |
| MD5: | 70E2BD4A5F6CC048F2037FB6DBF60F59 |
| SHA1: | 8957E9BEE99D6659F3E90744478B2DF01C2AFF7E |
| SHA-256: | 8E348CAD128DBD38F4DB072FAB87E66373848747408D99F35C10C36E325B8B0A |
| SHA-512: | 07BBA7B2A91C65D3AF8B7229AE82BF7481E50EDD8B3D0D8C550113B8CA28E108E6E9B12461C9F8617DECC6C66AF3ACBBE8145DD3A84F24B95799CAFDE1EB1C85 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 8P2701c72208k57cW4..aT808w5X8HuFD25K47M2mj9v0tv3Px51K69wHI496B7K188b3T37949159393t4uh47eTyC3b1N99R3nqpVOnnfZ09a8k06X8JS5O5kty55l68 r1Hk871fx50IL76a21Q1T..jMU279..xozN39F4G0g6Y6boq9QbFM2c8G4V2w0yauz4ig6IWQjv134uj1TQ26Hy0oH09979fw64nd2h63pR1..2Fx7kxpB..979b8Xq6F8 404p385C1Ima1023h..K8X5946J4480vBXo9i21nP4026Ujg25cVj403sldf7T48Wrt14Y9641613365949zub09XJW7..426Sl145187UBj8l93Y181ef3sl2s636kDi0zLPi4pU7su 8U080624Iza2rJ930eCQDVd748Ku7037Jn662U6..1Fs622Nf072Pp0u84tov5at90j0StS8jaD0k7BXd9JxWS333T50eMG1j63W236g4dSeiB8bzJ2.. |

| C:\Users\user\31956653\thjfdg.xcp | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 179166850 |
| Entropy (8bit): | 7.0277013788137745 |
| Encrypted: | false |
| SSDEEP: | 196608:epjpnpfpspOpIprp7pYpDpbppp4p4pmpEpgpnpmpCppp1pMpkptpxpWpbpKpzp4+:n |
| MD5: | 464F02264814F67FF065A76FB3BB221E |
| SHA1: | B98087AF04678AACC6F98F9400F07517A8064097 |
| SHA-256: | E853C69EC2723E99937524F06EA79ED700A9491174222605E951839F023DAE40 |
| SHA-512: | 89700BAC8A52B40EB3A8E0109D054B6C3E043B54B5AB9CD0048AA162C277906DDD0BEE61AB6A262CA12AA55F86D9585A271867F138A21E6A79558F3278F6BAC6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | ..;.....;.I.6e..O.6/y..ZK..p.....-w..`J.1B^^.d.pAx.gc.g..cq.l..N.......F.......nN..\.......#.c.s..M(T...........NWZ....p.u.2.1.6.6.6.c.Y.8.7.3.G.0.q.1.0.3.........9;.k*....N*.X..>`..aJ.........BF.....L ..&.mL._.8.H._....9.@.Z...O.J....;. U..g..!.....8./c.].s.....T...r..h../.3./.S.....-1...n.$\|.....h..$.....v/d../..9.5I>.!....{Y=.*..7..=<}..7gB..9.....a*..B]...d.....C.j....h&.U+...w.....2.s.0.7.P .5.P.e.5.2.Z.9.0.2.c.6.e.L.8.f.A.8.v.H.6.P.p.4.7.7.E.5.v.G.X.1.j.7.3.3.2.1.V.1.o.u.8.5.Q.....6.z.n.g.9.1.3.I.D.E.4.2.8.5.Z.6.K.e.B.6.9.n.p.J.2.R.6.2.I.1.0.f.u.i.Y.D.2.8.g.8.r.7.0.7 .5.7.....B.p.8.I.c.9.L.i.7.p.3.F.b.6.a.2.Y.....\.....]......Q...Ws...4.DJ.+..B.FI.V.].>#..f.....E....C.....V3....b.....Y.....D.....}J!A&.X..l...a....C./....t..%.])..$.Q,..z5..`.^.....q.F.u...5 ...*.....c.Z.6.I.0.3.6.7.3.1.N.x.5.0.1.4.L.p.k.j.3.....A.....+.A.O7.w.J.0..[d.wX.....-:W.C..PD....U....B..".....F^.G.....^P..!...(..!.C.8.g".&.M.h.*..h...Qx.g3KX.G..... |

| C:\Users\user\31956653\tlogpwsu.xml | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 506 |
| Entropy (8bit): | 5.465090732929896 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 7ECA9413CD44177EA404E1F3549D303B |
| SHA1: | 08AB492A0D375AC8DEBDA33A750E9703B2FAC1A5 |
| SHA-256: | 434D3D0A388D45DFD31F620784FE8224A75088A3F5130B78966196F5854CCF81 |
| SHA-512: | 013CFD2B36669F55A268C146742E3CFE3F430315F44F848EB78D071B4ECA36A0B99A56FDD5AAB116D48E65DE770C5AC5BF95CC2F39792E8669541FD82D618BE |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 8435r0Dx9kd4f90974GmL4EnbsVNEg6zmyh9e2Uaph0er3Yp14PzBMsVC94aKG407S012lC3tm8..e01Jf8A40ZwUSF4lLuQe004O31f4u657z14K4c73E857gV8dIKKR4 U70O8Q8F019O42707951N4q9a160FTig69e4yf37458QNR213878YP7Y5..816M94hi55WB248b90b81Hl71QlRe9lf32t8vn7983675zKCj33m564Jzo1rR3n41aRgO42 1OHUi54u46I0F931367Kf85mRh7993kthxAZZL0JUeT191OoP7H5Tp89p8Y7luT6EGHF1252215q2bl74gSF778f1b1j9W4..w4f38g796792687Mt648465M75V15742i 5t..uxJ0Z636DSy0V2bsgru..m0p55D4uc32UYMHfO91L7j7a123658X2l7257ok04ad50y55n5L1e66..4634H5E3jxa3p3RNKIxW5676DKI128En.. |

| C:\Users\user\31956653\ufrxn.msc | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 531 |
| Entropy (8bit): | 5.502780045827598 |
| Encrypted: | false |

**C:\Users\user\31956653\ufrxn.msc**

| | |
|---|---|
| SSDEEP: | |
| MD5: | 6074D095111C359480ACB96C9231F66F |
| SHA1: | 088A5DA089F1BD720B0F8E92A2D7A68F0488AE56 |
| SHA-256: | 3A413CDE1881BD4B2AEDE76034BAA94A00D40B6C7BDA18577636DCCBB7746CBA |
| SHA-512: | 3E7C1ABFCE67624A2B25CE4BB95429E70C4408CBA9BF92828F12A5B42F404BCFF6BA416A98D3AE30C2F64348946BA46560BC06B5F2B1B40A92007DF3B195A634 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 9069ka84619hQ4X1u61wbX1Ae3f2i9cWjUhIP759085HS93c8mQB7y4vb86Hh0G5m1yv6Br04215I38An0J1g74JyI4y03lWH3wZWH6RNnyCv94754..vV621X635k182g89nrT3T1..6960..0cNC93u78p7DvM408fp30W6186mMYHYlmb1d6GJZx9W5353ev8o578W98w1zNG9f1b9ds2Oz6..B254QI2031S1nJ0WZn21y488CmAJCl009S5CdI7xEu87heL0b46A7951E567c8FbCt0126z7qLpMxH6ofmB08Ka4..2896M652b3ov465PIW3Z0I8G861187..36xU3t0jp4862nJ2s6Z569549P2e245p51m2QPOc35v29ETw8H23xVt8U7321RSlw4S60h1N8tGG0VIBQ..MgQR35V89O56fj2886l3lpc706s1rK37q42E01g680fXgHAj2XIo6Vs3t3506a323cpUx9wgRzFE10K2w3963n1T8vFjZ30Cz9j6pZq.. |

**C:\Users\user\31956653\vdpstja.bin**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 654 |
| Entropy (8bit): | 5.466159936178476 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 1FC0F96F57264D51546177D2A6697CAF |
| SHA1: | 0056139558090B064B303817343B3917DAEC225B |
| SHA-256: | 32BB7294265BABD847D37D6D45F4DFFB60D3A9E12EA684417D2911A4380B8AA1 |
| SHA-512: | 87215809D30044A9D74E9B557DFDC1B3BC62DECA7C9B80BD0741C4849C951079C1FE2C525C7E2A9F70F2EB329BEA5B78CF2D6A5FA8425A64E075AFF88199D04 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 5M1Fej13so8K1ph807a6rU6go3991Kn1us5Lt69933e9XF2tM8Z..168lR7162pb5o8HZ55b94z31d663FO45q752Mg854qruZ9347T779..1o6275966u41M22Zw1H664j14KqC3K79tG53m4cSd218b2IbZ5U7o9755O2H2S1NP7620..5aW42Ci642D319UrW0pg3ro..16k028fLX2556n965HF8190sW233EML51U881Y9N69K575995271FKLOMB1KH6JoX18fJIX662X6C271jS5455e880D842gU..7V72MgW51Jw9Ox6wAC486g664c2u338n0xRxEk2Mu3whdM2x5DDAMqGGD1zTZ1IJSyW117r88oG07Me56uu5zO4v7CuvEA95pg6oAs613GsG61Y2zF8b86y6K..04h3xk567Y8GZcWIArS8795n6..N2Gzo7fg6720..8TbHsG4fRP6956D376cE1MGn29598858059aH3avA78y8RpJ285w13qyV408zT79qtv3j5619Ayyr23iuE6SX8l8pYphS66IZA2yC0fnD7H0T9aw207a84b0eR1278hR643P3VD5DS1FFv0PInq1852l4Q5fM04B05i87WV5B21rZqe15P24S7BV59.. |

**C:\Users\user\31956653\vmwepitk.ico**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 518 |
| Entropy (8bit): | 5.446951342718582 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 3BC051ABDDADF20F44239A3F4D7729A2 |
| SHA1: | 85907AB13C191D6EA676205B2013FB4B2D76D700 |
| SHA-256: | 1A458064D0C494B97DBA9BA3B3B815D1E4457672AD982D234F4CCDE1A834087F |
| SHA-512: | 939DCFA24EB6A42412BA2D2DA4158543CEC96CCDF010A09C739684805464604805AB6B145C573BDF3C0591D4CDBFB260363632AED9383AB17DF028DAD81614F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | h4y74215M7N98ioB3K66CwgPHQ7n8bM40Q9w09m75996T8S5l93197feabk86Asj60v1b03in68H568OJJaX82305t00MscLTi6I2y903578V6E44v513liRSMG6j5P..65Uii857pu51gT292r6571R2s3pM656h4NH4eZX3461cF72c88c5X32s3baF6SAI8Z9tm9Ht9UXXO97Sq7gv4g274985boZ464H0399S5Ft8BX7qY5xm1C..Ix682Z99m9G..17y9678VM0R4fbzO0yii35j84ZHrz7QGq6800Pu28krPP2DW06329cXj5z4HnG10u5R7Eb65..me741b7t39VAN6rJ8cU8T8Y1g979686721m6t0Rh3Al733KNxXwr8328ZJaWzX67202y456zAp5diV284725l6qs0134n5fT9c3F16Ik0Iz7PQ65IvX..5V6647SD6I7627Y3l2G83465rcO99bKG1s5H37BkKe4T8210K00x65YJE7473F3.. |

**C:\Users\user\31956653\vxnslrtcv.docx**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 595 |
| Entropy (8bit): | 5.498200602093174 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | CE89B449E0BF13583FCF623DC39E4A3A |

| C:\Users\user\31956653\vxnslrtcv.docx | |
|---|---|
| SHA1: | 5AF6F11E0E2D583FDD0B8EF96BDB1AB5B8516FD7 |
| SHA-256: | 7D79C01E5A34AE5BB59F40F23BF1545EFD01760803551FFA744769FE9098FF34 |
| SHA-512: | D99542FEFA2C5DE4EA1F0B290B462BE35E7BF161FB77F751E8FB25E5B95B74CFE01C72FC95EF08909974EF9053CE028FBCDEBED0DA4C123BF29D09C034FFC(<br>25 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | lJ1l125B03rJ9T7is4bPP6Q6XMi248S54V58iX4j3Y3C01N0Lec371w70P6sgeyh2e03775B9D8r63G6Y35520d807b5cW55732Vk24N833..C2E7vl7390701H..wG949<br>5x78A3uV43h3NI..o4NG3y1166O06iAmx9l0g..Mx8FsQ088H5E0qlim4Ja100e9h3YKh5j798D4Xsp2se961Z4e0CdY25n1R9OuV3ua062tQ6K7o31T25Di772Q8W8294<br>InYh77jKIXZwx31464j98h55L5w7wj..dEU7698St7YOU5Kh5H4d05765jV8G9049nX803ry7U2fNN074K960HKJ1722E7vOD03Od5x45uUh6Pq..0lVn8Q169569l3398<br>4TH341t8r26UjzH5N828Kt1pqK665y2b3H4M43a29QP42YW3yy8zn6LHR1UQYJ58Qd95qKPM94LQXa4887XRP..32PapR7p7T7w559B64fb0k3C4Cu8Bm2xK<br>1424E9108F0p79aL2Z6sUfbEhF9C24GIWR6QIRT19u4Sth9758c6r356Xy3s35mIF6b7T5ns2Z0C7X9pV38.. |

| C:\Users\user\31956653\whgh.dll | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 563 |
| Entropy (8bit): | 5.410246118862809 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | F9DCC92A013B1A4B704BD50130EDA877 |
| SHA1: | 629A854A96C2020E0C07D9EFF31B9F95BBB5DC6B |
| SHA-256: | C1E1AD8AF0A12CD3AAA7C9FB348FE0A5B98106C3044F2338CD3BC0830187B98F |
| SHA-512: | 196773F45D02654198D0FBD22C384358B13C3536ADDA41CFB2A4D0B1B0664BC202BFA32F03F3AB6D894E931FF4B74CD58DF53197781C0BE6CFB1A53F141A61D |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | d38t2ll882p3m6286AT7epu1o3WO1vfiS66f3X0JITm6k40TSPr995wGR4U18E53235Q0GdW261e8q3MFR7X901i15Z910..935120c20f1NCeTP130YI58f0N09K693eD<br>5y2Y37X33N77h8Bx5n3U57XGNY493Ap703S6CFcS1Yeb59vEo27..a9w5D1x9Wk878ymu5P65Mha37Z6VS07l6D4Y13rQ458245jlvCfN38rGTjgsunmU8GlL89eH9495v<br>Cq6cCK7kkl93r64e9vL03a60eQ4ik136wf05L3Ce27893z8K4jn5Mo9G0l4L71y9..10J9k71LwlE04357715ol4nH..938CB3n8uy95H532el5962Gc6a500G32qC25P3<br>19048a50Piu5957Qdz6ue861z23425OcG8fMYi9b4bTJGk9z5445n7fte51j3392057fde2th7053E8o2s73Lh5K0d86557..l218O9mil006clv3C4j84K327wD6253u8EX7Kn0c7i7<br>563o95V72L0BUKf94S7UA36t368cTq1.. |

| C:\Users\user\31956653\xdotxo.docx | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 517 |
| Entropy (8bit): | 5.466351604074262 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 49E7CBE3D9F1AC75C33159FFD823EB1E |
| SHA1: | CE297374AC9139763C4F42EDFCAA24148267681B |
| SHA-256: | 323B5E48259C5E894A23BE28A5DEFCEA8A9DE7C09CAB11CD471B73A016408441 |
| SHA-512: | 68D14282E48C130284E2AF41E69BB99C0548CA2B93675FE450E6BAAC1EA1719C94F1E95FF78447FF5B4FB4E7C5C5E2867D9641F52C1465A2B7C9B9A18424BC3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 35mc101735L06Rh3A08poM8Tt1Q4n4g72k8j793c9248rhp556H0dAU26N0qxC8C4c8AoZ97Gvg5PHc99Khu9EK9wVa08Uh8K288LBt9721DB49R87qKAS13vB94Td9YA.<br>.6ooCO01A5h7m11r508S7WW07..1439X2s05Awv3X7sB0Te34S737EP6785sY329H..18q80N9de5G5I79mBZ1Po2701U2N5DLnR38KlN0Jq40X52AJr3S3cAEy8k0w758<br>R0TcQ361gO57KH45V760o..2422MkH58CZbNBv7DKo4W299NWILKg47oR28A1Z8yL20..L2AHdHWT82KA3P31RiBeN28093SF727Y4H9CX475Mt13dE3nms2<br>A5x..S3nENqOGVd7Gl290177o69Q019XUl9L415y2jmag389V6kis3WQlZ883T3kG625H5669o9VtUGY8s8q7s700Dx38r5Sv84H079GL3f09C0nYp6X24G6172C3b2C7M<br>0LF34.. |

| C:\Users\user\31956653\xmjk.pif | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 776432 |
| Entropy (8bit): | 6.353910854155555 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 279DAE7236F5F2488A4BACDE6027F730 |
| SHA1: | 29A012E5259739F24480CEDFD6D5F2D860CFCDB3 |
| SHA-256: | 415850F2706681A6D80708FCA8AC18DCF97E58B8F3FDC7BC4B558AB15FC0A03F |
| SHA-512: | B81276FC4D915A9721DAE15AA064781A1DBA665FF4864CCBDF624E8049C1B3C12A2B374F11CFFCF6E4A5217766836EDBC5F2376FFA8765F9070CBD87D7AE2FI<br>8 |
| Malicious: | **true** |

| C:\Users\user\31956653\xmjk.pif | |
|---|---|
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: Metadefender, Detection: 37%, Browse<br>• Antivirus: ReversingLabs, Detection: 56% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich.....PE..L....%O....."..... .....d..... ....@.....0.....Jg....@...@.....@.....T.....c..... ..D.....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...D.....@..B..... |

| C:\Users\user\31956653\xowesno.icm | |
|---|---|
| Process: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 630 |
| Entropy (8bit): | 5.469657756184613 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 82A2AA44DA9BE298E7CA6F9B1BE37489 |
| SHA1: | 951CBE31A533D075F9981148061A5E39DF4D8ECF |
| SHA-256: | D1C0DB29168FBB45315E6897FD03B91C7B7D452C8B363BA17BA7D723A5C858EA |
| SHA-512: | 9A1FB6140BF8B45197F295B2EAD678D02F957660A7DF4CE1F0F30E41EC07AE43331ADA081F0EDCAED1AA62AE8EE4CEB38ECE90A323432DD982467F3152D00D3F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 6P35vaP7iS2cbly5tn56D78h6983t7I7531dSXgRf4w21070Po10FjxmL7FS9m5X96JXw1M5515l84Q1vVya9283o12826077FQX13f..791R191QGC73ef6941W09io8pg372fJ4p5YoNfM000E1WGjn24V63N80gm851ZpYoB153W3E6407r2d7606362301wU6qH213Y..110T8j870q1B1xm3YU6a0141c2Kg873ZpUE4kdw0tKR465dH92W6..9kfd41F5Vqf00504914O900484NvD184u9K34x57VODzJZ4216X5a4IZ964645332IV6j3QJgm0Rc1hM7c9O2g93V9p60sfIP1dZ0l7XgH031qgKUYA4tGn45W6bF0Lb274K3l7Z8..r1e840v3fu0N03v565VB26Mdo31OpX5r47cA01f68sAkm7W9tRA5c178I97F1u96zd5n1GY590B2031308Z8zClMP7..34K14827mq2QMBR3Q4v8MYHz0Sp1K05vIWR3573E99xnFUkyz2wrt1R830707csLT1abklg22eJqZ466U74L7fH7cL2bftMG66o214Z5Cs3S17c46A46nXYL67w5Pa1PG83Fz7702a.. |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 142 |
| Entropy (8bit): | 5.090621108356562 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 8C0458BB9EA02D50565175E38D577E35 |
| SHA1: | F0B50702CD6470F3C17D637908F83212FDBDB2F2 |
| SHA-256: | C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53 |
| SHA-512: | 804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0.. |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log | |
|---|---|
| Process: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 142 |
| Entropy (8bit): | 5.090621108356562 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 8C0458BB9EA02D50565175E38D577E35 |
| SHA1: | F0B50702CD6470F3C17D637908F83212FDBDB2F2 |
| SHA-256: | C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53 |
| SHA-512: | 804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0.. |

| C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
|---|

| C:\Users\user\AppData\Local\Temp\RegSvcs.exe | |
|---|---|
| Process: | C:\Users\user\31956653\xmjk.pif |
| File Type: | PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 45152 |
| Entropy (8bit): | 6.149629800481177 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 2867A3817C9245F7CF518524DFD18F28 |
| SHA1: | D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC |
| SHA-256: | 43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50 |
| SHA-512: | 7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D<br>B42 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Metadefender, Detection: 0%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ..... ..H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]... |

| C:\Users\user\AppData\Local\Temp\tmp7982.tmp | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1308 |
| Entropy (8bit): | 5.107159514403738 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 211C08A48B92E556A855FB90EE4B0942 |
| SHA1: | 4E3ECFBEA0CCA0EE2743C0E23ED3FC79EB2E282A |
| SHA-256: | 21F529F720EE77AD03AFD3CFA4CE04EBAF243C3E752F14C268529665CA936146 |
| SHA-512: | B65C55C05249DFFFD0B52DF66DBA692CE21B6D447DEA43E93DACE718E40ABAC069A6BD2DC4CF0BC3F979A327BB7896BE6A3A36540916A33E0CDA8B974E295<br>5F1 |
| Malicious: | **true** |
| Reputation: | unknown |
| 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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak |

| C:\Users\user\AppData\Local\Temp\tmp7CDE.tmp | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1310 |
| Entropy (8bit): | 5.109425792877704 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 5C2F41CFC6F988C859DA7D727AC2B62A |
| SHA1: | 68999C85FC7E37BAB9216E0099836D40D4545C1C |
| SHA-256: | 98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B |
| SHA-512: | B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 |
| Malicious: | false |
| Reputation: | unknown |
| 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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | Non-ISO extended-ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | AC8BC54500409DC48009947C7192C04F |
| SHA1: | 6929BE6CFA0169258B2870A14CA8E7F80CC3183B |
| SHA-256: | 96A15B672AA0CA305E924C7EF126ED25863728FA7778B4558D3B29003DE0CD32 |
| SHA-512: | 31D6F483C75A42A4782386C00AABEFFC6A138E5C06ACAC1A63FA1CBA0507CB1A09627BC0B94C96162055160B6200BCAC49EF53BF092B7F3606238D7A2CA9CD3 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | oc.R...H |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat | |
|---|---|
| Process: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 45 |
| Entropy (8bit): | 4.4112044189276585 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 4879007AC97C3DF41896D937852ABBE7 |
| SHA1: | 05A8C8638A4C8157216EF4AE24B43D3A4E750F00 |
| SHA-256: | 18B03E2D9F5F5E7E26686848D71049AC56D06500A2AB420A3A01CA0ED6C7AD18 |
| SHA-512: | 03C80EC22591301B32EB0310A188B1C4C24DC16BF9E2E25B22A95AA6E36E9B7002196B13A522F36D9AC64C38A98D6BA06C3387DBBE7CB3319E45BC43359A6C3 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |

| C:\Users\user\temp\eblsq.ppt | |
|---|---|
| Process: | C:\Users\user\31956653\xmjk.pif |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 80 |
| Entropy (8bit): | 4.988137789834391 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | FE5D5426B0972408E1424ABC0F49F71B |
| SHA1: | A994F74A16522DAF1DDC270605C1B88979ABBCAD |
| SHA-256: | 35A80327293D6268AA1C1FA881C3E84AF272B297672458C2CB3CACC41AFA691E |
| SHA-512: | 2EB9191B629B025775F4CDA31F64FDC99A26E7A98AAAA94EC1C956AF719CE067A5545A0B0E37E178BDAD87734924C130B521EAB2E8FB23DC1952334660ACB6B |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | [S3tt!ng]..stpth=%userprofile%..Key=Chrome..Dir3ctory=31956653..ExE_c=xmjk.pif.. |

| \Device\ConDrv | |
|---|---|
| Process: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| File Type: | ASCII text, with CRLF, LF line terminators |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 4.911407397013505 |
| Encrypted: | false |
| SSDEEP: | |
| MD5: | 623152A30E4F18810EB8E046163DB399 |
| SHA1: | 5D640A976A0544E2DDA22E9DF362F455A05CFF2A |
| SHA-256: | 4CA51BAF6F994B93FE9E1FDA754A4AE74277360C750C04B630DA3DEC33E65FEA |
| SHA-512: | 1AD53476A05769502FF0BCA9E042273237804B63873B0D5E0613936B91766A444FCA600FD68AFB1EF2EA2973242CF1A0FF617522D719F2FA63DF074E118F370B |
| Malicious: | false |

| \Device\ConDrv | |
|---|---|
| Reputation: | unknown |
| Preview: | Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation.  All rights reserved.....The following installation error occurred:..1: Assembly not found: '0'... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.836743207281609 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | dAkJsQr7A9.exe |
| File size: | 1103745 |
| MD5: | b115228fe5e180f505c081aa829c1a86 |
| SHA1: | c242c6a90ae569e55ed6acdb5c765244f623b9b6 |
| SHA256: | a64c1b956bb79c5cfec594165a4ba37e9f695f8f83ec2b7bc2729d19c2598cd5 |
| SHA512: | c7b49a9fdbd08e0eb219758c8d8b44bd0b43663d66053bc52068edfa6efaf70a809218995dda2eec5e2414e2dc96385236c991300293b617d1da022f02593620 |
| SSDEEP: | 24576:rAOcZEh2G8ydrzUcNV53O9QblBWTq6ai0bagi7vzJL:tBNlw2x+Qbl8Tq6d4a5vN |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y..../y..#...&...,...._.....`_.'...._f.'...._..'.. |

## File Icon

| | |
|---|---|
| Icon Hash: | b491b4ecd336fb5b |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x41e1f9 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE |
| DLL Characteristics: | TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 1 |
| File Version Major: | 5 |
| File Version Minor: | 1 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 1 |
| Import Hash: | fcf1390e9ce472c7270447fc5c61a0c1 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x30581 | 0x30600 | False | 0.589268410853 | data | 6.70021125825 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x32000 | 0xa332 | 0xa400 | False | 0.455030487805 | data | 5.23888424127 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x3d000 | 0x238b0 | 0x1200 | False | 0.368272569444 | data | 3.83993526939 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .gfids | 0x61000 | 0xe8 | 0x200 | False | 0.333984375 | data | 2.12166381533 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x62000 | 0x4c28 | 0x4e00 | False | 0.602263621795 | data | 6.36874241417 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x67000 | 0x210c | 0x2200 | False | 0.786534926471 | data | 6.61038519378 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States |  |

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 10/12/21-12:35:17.105237 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 56527 | 8.8.8.8 | 192.168.2.3 |
| 10/12/21-12:35:27.793788 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 63297 | 8.8.8.8 | 192.168.2.3 |
| 10/12/21-12:35:49.817168 | UDP | 254 | DNS SPOOF query response with TTL of 1 min. and no authority | 53 | 50585 | 8.8.8.8 | 192.168.2.3 |

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Oct 12, 2021 12:34:39.230012894 CEST | 192.168.2.3 | 8.8.8.8 | 0xa4c | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:34:50.479154110 CEST | 192.168.2.3 | 8.8.8.8 | 0x58ab | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:34:55.622173071 CEST | 192.168.2.3 | 8.8.8.8 | 0xbb40 | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:17.085382938 CEST | 192.168.2.3 | 8.8.8.8 | 0x43bb | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:22.561073065 CEST | 192.168.2.3 | 8.8.8.8 | 0x608d | Standard query (0) | strongodss.ddns.net | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Oct 12, 2021 12:35:27.773935080 CEST | 192.168.2.3 | 8.8.8.8 | 0x600b | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:49.796987057 CEST | 192.168.2.3 | 8.8.8.8 | 0x64ec | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:55.119167089 CEST | 192.168.2.3 | 8.8.8.8 | 0x8c85 | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:36:00.383613110 CEST | 192.168.2.3 | 8.8.8.8 | 0x52df | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:36:21.926038980 CEST | 192.168.2.3 | 8.8.8.8 | 0x5a76 | Standard query (0) | strongodss .ddns.net | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Oct 12, 2021 12:34:39.248326063 CEST | 8.8.8.8 | 192.168.2.3 | 0xa4c | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:34:50.497493029 CEST | 8.8.8.8 | 192.168.2.3 | 0x58ab | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:34:53.358833075 CEST | 8.8.8.8 | 192.168.2.3 | 0x83cc | No error (0) | windowsupdate.s.llnwi.net | | 178.79.242.0 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:34:55.640309095 CEST | 8.8.8.8 | 192.168.2.3 | 0xbb40 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:17.105237007 CEST | 8.8.8.8 | 192.168.2.3 | 0x43bb | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:22.577892065 CEST | 8.8.8.8 | 192.168.2.3 | 0x608d | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:27.793787956 CEST | 8.8.8.8 | 192.168.2.3 | 0x600b | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:49.817167997 CEST | 8.8.8.8 | 192.168.2.3 | 0x64ec | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:35:55.138731003 CEST | 8.8.8.8 | 192.168.2.3 | 0x8c85 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:36:00.402153969 CEST | 8.8.8.8 | 192.168.2.3 | 0x52df | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 12:36:21.944379091 CEST | 8.8.8.8 | 192.168.2.3 | 0x5a76 | No error (0) | strongodss .ddns.net | | 185.19.85.175 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: dAkJsQr7A9.exe PID: 6308 Parent PID: 3652

#### General

| | |
|---|---|
| Start time: | 12:34:10 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\Desktop\dAkJsQr7A9.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\dAkJsQr7A9.exe' |
| Imagebase: | 0xca0000 |
| File size: | 1103745 bytes |
| MD5 hash: | B115228FE5E180F505C081AA829C1A86 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: xmjk.pif PID: 6660 Parent PID: 6308

### General

| | |
|---|---|
| Start time: | 12:34:23 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\31956653\xmjk.pif |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\31956653\xmjk.pif' thjfdg.xcp |
| Imagebase: | 0x3f0000 |
| File size: | 776432 bytes |
| MD5 hash: | 279DAE7236F5F2488A4BACDE6027F730 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350179976.000000000449A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350063292.0000000004431000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350063292.0000000004431000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350063292.0000000004431000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352276623.00000000044CE000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352276623.00000000044CE000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352276623.00000000044CE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352230581.00000000044CE000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352230581.00000000044CE000.00000004.00000001.sdmp, Author: Joe Security |

| | |
|---|---|
| | • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352230581.00000000044CE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352180992.0000000004466000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352180992.0000000004466000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352180992.0000000004466000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352056687.000000000449A000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352056687.000000000449A000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352056687.000000000449A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.351507345.0000000004503000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.351507345.0000000004503000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.351507345.0000000004503000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350312058.0000000004431000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350312058.0000000004431000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350312058.0000000004431000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350212865.0000000003748000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350212865.0000000003748000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350212865.0000000003748000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350502878.0000000004503000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350502878.0000000004503000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350502878.0000000004503000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.350252312.0000000004466000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.350252312.0000000004466000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.350252312.0000000004466000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352384580.0000000004431000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352384580.0000000004431000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352384580.0000000004431000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.352498016.0000000003748000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.352498016.0000000003748000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.352498016.0000000003748000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Antivirus matches: | • Detection: 100%, Joe Sandbox ML<br>• Detection: 37%, Metadefender, Browse<br>• Detection: 56%, ReversingLabs |
| Reputation: | low |

## File Activities

Show Windows behavior

### File Created

### File Written

### File Read

## Registry Activities

Show Windows behavior

### Key Value Created

# Analysis Process: RegSvcs.exe PID: 5792 Parent PID: 6660

## General

| | |
|---|---|
| Start time: | 12:34:31 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| Imagebase: | 0x720000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| 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: 00000006.00000002.581022172.00000000060B0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.581022172.00000000060B0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.581022172.00000000060B0000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.576672734.0000000002EE1000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.573655036.0000000000B02000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.573655036.0000000000B02000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000006.00000002.573655036.0000000000B02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.580231784.00000000057C0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.580231784.00000000057C0000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.579331613.0000000003F29000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000006.00000002.579331613.0000000003F29000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.580427027.0000000005900000.00000004.00020000.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.580427027.0000000005900000.00000004.00020000.sdmp, Author: Florian Roth |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |
| Reputation: | high |

## File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

## Analysis Process: schtasks.exe PID: 7124 Parent PID: 5792

### General

| | |
|---|---|
| Start time: | 12:34:36 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7982.tmp' |
| Imagebase: | 0xa10000 |
| 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: 6936 Parent PID: 7124

### General

| | |
|---|---|
| Start time: | 12:34:36 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: schtasks.exe PID: 6760 Parent PID: 5792

### General

| | |
|---|---|
| Start time: | 12:34:37 |

| | |
|---|---|
| Start date: | 12/10/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp7CDE.tmp' |
| Imagebase: | 0xa10000 |
| 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: RegSvcs.exe PID: 6312 Parent PID: 664

### General

| | |
|---|---|
| Start time: | 12:34:37 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 |
| Imagebase: | 0x690000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| 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 Written**

**File Read**

## Analysis Process: conhost.exe PID: 6580 Parent PID: 6760

### General

| | |
|---|---|
| Start time: | 12:34:37 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: conhost.exe PID: 6560 Parent PID: 6312

### General

| | |
|---|---|
| Start time: | 12:34:37 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: xmjk.pif PID: 6848 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 12:34:38 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\31956653\xmjk.pif |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp |
| Imagebase: | 0x3f0000 |
| File size: | 776432 bytes |
| MD5 hash: | 279DAE7236F5F2488A4BACDE6027F730 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: dhcpmon.exe PID: 7096 Parent PID: 664

### General

| | |
|---|---|
| Start time: | 12:34:39 |
| Start date: | 12/10/2021 |
| Path: | C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 |
| Imagebase: | 0x7f0000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Antivirus matches: | • Detection: 0%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |

### File Activities

Show Windows behavior

#### File Created

#### File Written

File Read

## Analysis Process: conhost.exe PID: 7112 Parent PID: 7096

### General

| | |
|---|---|
| Start time: | 12:34:40 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: xmjk.pif PID: 4356 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 12:34:41 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\31956653\xmjk.pif |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp |
| Imagebase: | 0x3f0000 |
| File size: | 776432 bytes |
| MD5 hash: | 279DAE7236F5F2488A4BACDE6027F730 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.394776495.0000000004C6A000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.394776495.0000000004C6A000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.394776495.0000000004C6A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.394077058.0000000003EA4000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.394077058.0000000003EA4000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.394077058.0000000003EA4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.395083059.0000000004C36000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.395083059.0000000004C36000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.395083059.0000000004C36000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.392253067.0000000004CD4000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.392253067.0000000004CD4000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.392253067.0000000004CD4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: |

00000014.00000003.391774753.0000000004C36000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391774753.0000000004C36000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391774753.0000000004C36000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391477356.0000000004C9F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391477356.0000000004C9F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391477356.0000000004C9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391366953.0000000004C36000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391366953.0000000004C36000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391366953.0000000004C36000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.392467054.0000000004D08000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.392467054.0000000004D08000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.392467054.0000000004D08000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.395194489.0000000004C01000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.395194489.0000000004C01000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.395194489.0000000004C01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391714719.0000000004C6A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391714719.0000000004C6A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391714719.0000000004C6A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.394033269.0000000004D08000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.394033269.0000000004D08000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.394033269.0000000004D08000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391833117.0000000004C9F000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391833117.0000000004C9F000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391833117.0000000004C9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391948004.0000000004CD4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391948004.0000000004CD4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391948004.0000000004CD4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.391514426.0000000004C01000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.391514426.0000000004C01000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000003.391514426.0000000004C01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.392573341.0000000004D3C000.00000004.00000001.sdmp, Author:

| | |
|---|---|
| | Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.392573341.0000000004D3C000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.392573341.0000000004D3C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.394945613.0000000004CD3000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.394945613.0000000004CD3000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.394945613.0000000004CD3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000003.394535307.0000000004C9F000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000003.394535307.0000000004C9F000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000014.00000003.394535307.0000000004C9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |

### File Activities

Show Windows behavior

#### File Deleted

#### File Written

#### File Read

## Analysis Process: wscript.exe PID: 6420 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 12:34:48 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\wscript.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\System32\WScript.exe' 'C:\Users\user\31956653\Update.vbs' |
| Imagebase: | 0x7ff752ac0000 |
| File size: | 163840 bytes |
| MD5 hash: | 9A68ADD12EB50DDE7586782C3EB9FF9C |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

## Analysis Process: xmjk.pif PID: 4608 Parent PID: 6420

### General

| | |
|---|---|
| Start time: | 12:34:50 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\31956653\xmjk.pif |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp |
| Imagebase: | 0x3f0000 |
| File size: | 776432 bytes |
| MD5 hash: | 279DAE7236F5F2488A4BACDE6027F730 |
| Has elevated privileges: | false |
| Has administrator privileges: | false |

| | |
|---|---|
| Programmed in: | C, C++ or other language |

## Analysis Process: RegSvcs.exe PID: 5572 Parent PID: 4356

### General

| | |
|---|---|
| Start time: | 12:34:51 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\RegSvcs.exe |
| Imagebase: | 0x7f0000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| 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: 00000019.00000002.418761309.0000000004479000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000019.00000002.418761309.0000000004479000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.418519690.0000000003471000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000019.00000002.418519690.0000000003471000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.415517736.0000000000BC2000.00000040.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.415517736.0000000000BC2000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000019.00000002.415517736.0000000000BC2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |

## Analysis Process: xmjk.pif PID: 3412 Parent PID: 6420

### General

| | |
|---|---|
| Start time: | 12:34:52 |
| Start date: | 12/10/2021 |
| Path: | C:\Users\user\31956653\xmjk.pif |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\31956653\xmjk.pif' C:\Users\user\31956653\thjfdg.xcp |
| Imagebase: | 0x3f0000 |
| File size: | 776432 bytes |
| MD5 hash: | 279DAE7236F5F2488A4BACDE6027F730 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411798480.0000000003E28000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411798480.0000000003E28000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411798480.0000000003E28000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net><br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.412888978.0000000003E28000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.412888978.0000000003E28000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.412888978.0000000003E28000.00000004.00000001.sdmp, Author: |

Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411513032.0000000003D56000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411513032.0000000003D56000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411513032.0000000003D56000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411892507.0000000003E5C000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411892507.0000000003E5C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411892507.0000000003E5C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.414829262.0000000003D56000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.414829262.0000000003D56000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.414829262.0000000003D56000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411602320.0000000003DBF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411602320.0000000003DBF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411602320.0000000003DBF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.412949182.00000000005A6000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.412949182.00000000005A6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.412949182.00000000005A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.414560875.0000000003DF3000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.414560875.0000000003DF3000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.414560875.0000000003DF3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411727538.0000000003DF4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411727538.0000000003DF4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411727538.0000000003DF4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.414304073.0000000003D8A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.414304073.0000000003D8A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.414304073.0000000003D8A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.413709722.0000000003DBF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.413709722.0000000003DBF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.413709722.0000000003DBF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411158873.0000000003D56000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411158873.0000000003D56000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411158873.0000000003D56000.00000004.00000001.sdmp, Author:

Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411291828.0000000003DBF000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411291828.0000000003DBF000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411291828.0000000003DBF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411683482.0000000003DF4000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411683482.0000000003DF4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411683482.0000000003DF4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411424843.0000000003D8A000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411424843.0000000003D8A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411424843.0000000003D8A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.415163976.0000000003D21000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.415163976.0000000003D21000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.415163976.0000000003D21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000003.411346377.0000000003D21000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000003.411346377.0000000003D21000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000001B.00000003.411346377.0000000003D21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

# Disassembly

## Code Analysis