**ID:** 502665
**Sample Name:** niPie.exe
**Cookbook:** default.jbs
**Time:** 08:36:49
**Date:** 14/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

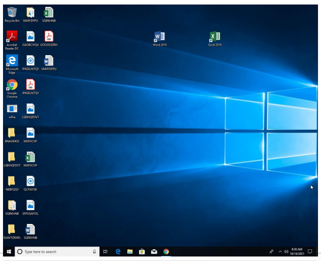
# Windows Analysis Report niPie.exe

## Overview

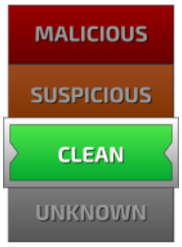
### General Information

| | |
|---|---|
| Sample Name: | niPie.exe |
| Analysis ID: | 502665 |
| MD5: | 601fda01efb1a22.. |
| SHA1: | 925f30c4a425c13.. |
| SHA256: | 5020bbc58ef082a. |
| Infos: | |

Most interesting Screenshot:



### Detection

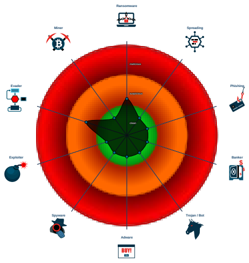


| | |
|---|---|
| Score: | 4 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

- Uses 32bit PE files
- Found evasive API chain (may stop…
- Sample file is different than original …
- Contains functionality to dynamically…
- Found large amount of non-executed…
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Detected potential crypto function

### Classification



## Process Tree

- **System is w10x64**
- niPie.exe (PID: 6404 cmdline: 'C:\Users\user\Desktop\niPie.exe' MD5: 601FDA01EFB1A22E18A19793158B51FE)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Jbx Signature Overview

Click to jump to signature section

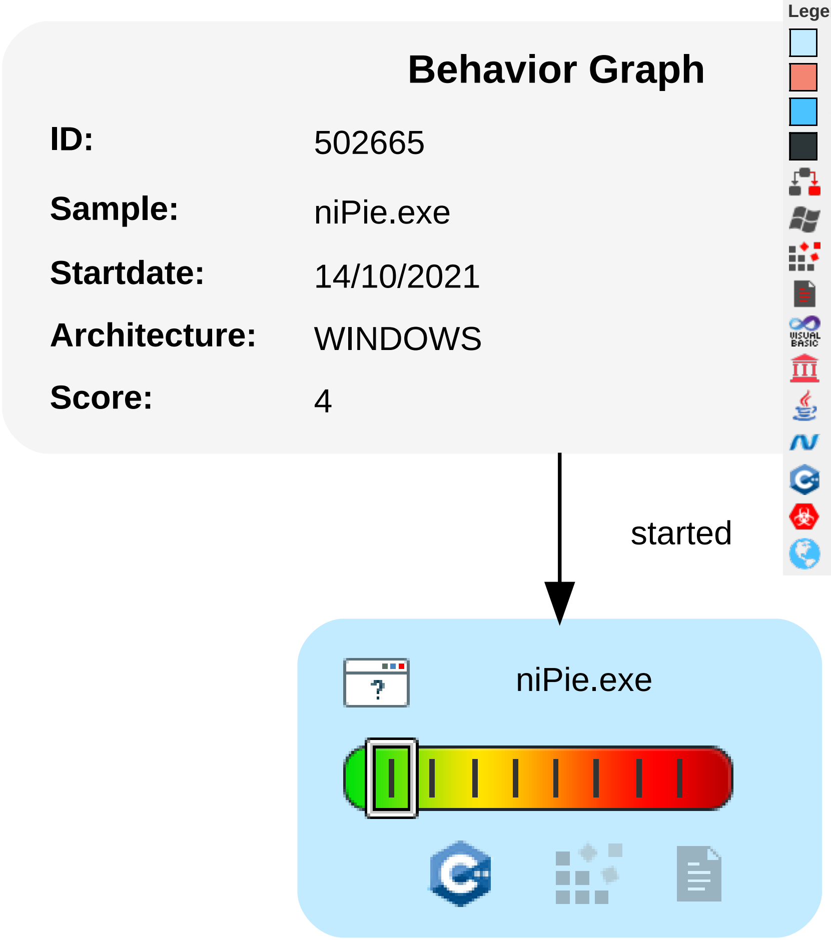
There are no malicious signatures, click here to show all signatures.

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Command and Scripting Interpreter 2 | Path Interception | Path Interception | Obfuscated Files or Information 1 | OS Credential Dumping | File and Directory Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Native API 1 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | System Information Discovery 2 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |

## Behavior Graph

Hide Legend



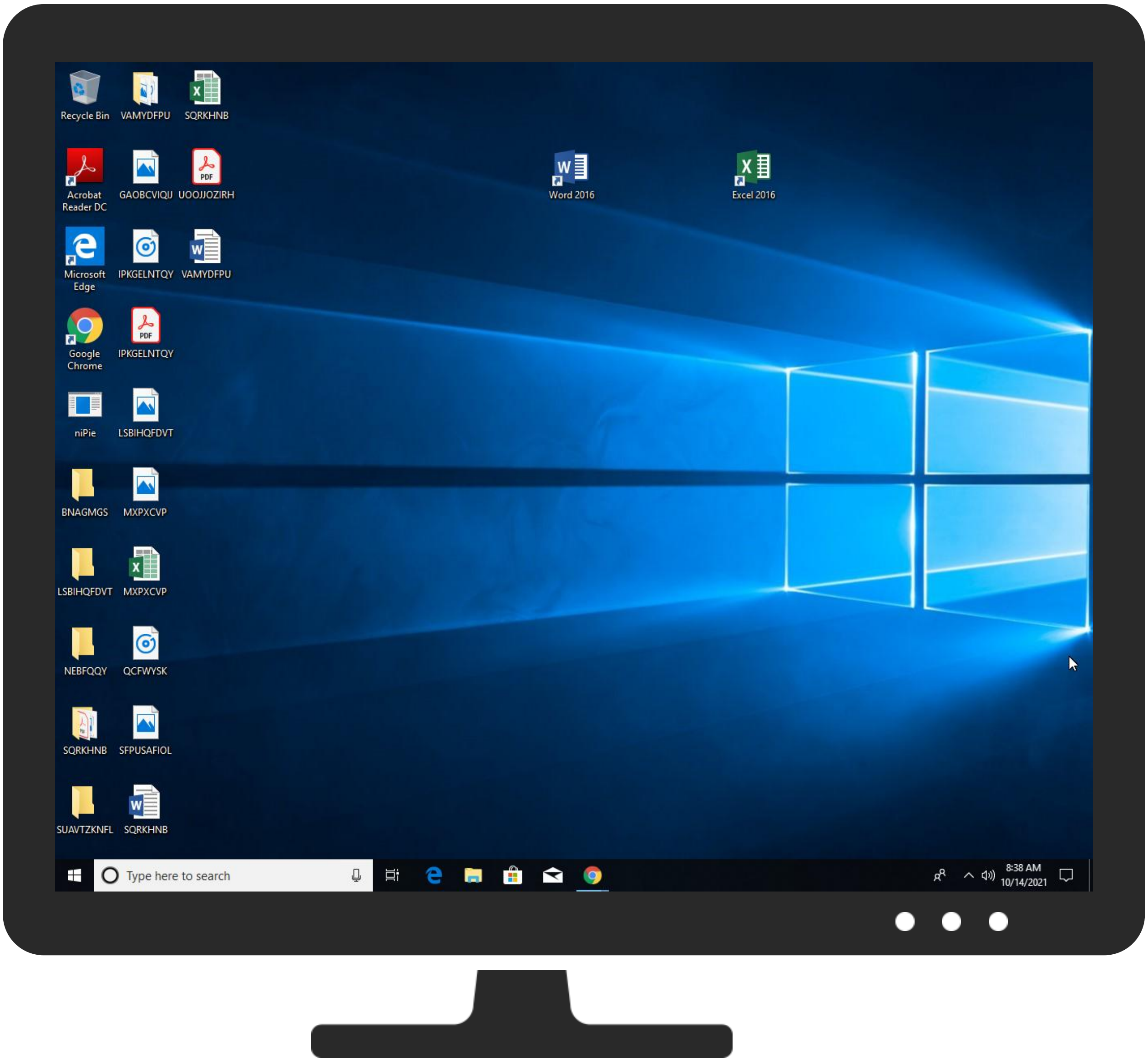
**Legend:**

- 🟦 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

## 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 |
|---|---|---|---|---|
| niPie.exe | 0% | Virustotal | | Browse |
| niPie.exe | 0% | Metadefender | | Browse |
| niPie.exe | 0% | ReversingLabs | | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

**No Antivirus matches**

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ocsp.thawte.com0 | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## URLs from Memory and Binaries

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 502665 |
| Start date: | 14.10.2021 |
| Start time: | 08:36:49 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 2m 50s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | niPie.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: | 5 |
| 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: | CLEAN |
| Classification: | clean4.winEXE@1/0@0/0 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 100% (good quality ratio 97.2%)<br>• Quality average: 87.1%<br>• Quality standard deviation: 22.3% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

**No created / dropped files found**

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 5.892836892157124 |
| 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: | niPie.exe |
| File size: | 73664 |
| MD5: | 601fda01efb1a22e18a19793158b51fe |
| SHA1: | 925f30c4a425c133915ee92dd4c0900f31536c04 |
| SHA256: | 5020bbc58ef082a5ac8e42e394c4235e88b9c5bd1ed3cdc126a24a649997ebf3 |
| SHA512: | 0db9ac45dfa3e4530fa4a945e3cac301e1ee8b26fc2690739741d72e1b7712e205f4bf83463e51c70df141af663ffa54c4e281d93f3bc386487a42eb1778a03c |
| SSDEEP: | 768:gjan8GnhwDHcnrkqAAO8IEwm8iNWTGzvtKsDsoxm3whvI:gjanoDGrkbAO80mhN/ZKsDnmghw |
| File Content Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$......./..)k..zk..zk..z...zh..z...zx..z...zW..z...zc..z2..zl..zk..z,..zm..zo..z...zj..z...zj..zRichk..z................PE..L...j.l>... |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x402d93 |
| 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: | |
| Time Stamp: | 0x3E49816A [Tue Feb 11 23:04:10 2003 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: | 8fcbb82d712dc622f705d3815ebb3266 |

### Authenticode Signature

| | |
|---|---|
| Signature Valid: | **true** |
| Signature Issuer: | CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US |
| Signature Validation Error: | **The operation completed successfully** |
| Error Number: | 0 |
| Not Before, Not After | • 4/11/2016 5:00:00 PM 7/12/2019 4:59:59 PM |
| Subject Chain | • CN=National Instruments Corporation, O=National Instruments Corporation, L=Austin, S=Texas, C=US |
| Version: | 3 |
| Thumbprint MD5: | 1C8D1A5469552A41DE716974A986D673 |
| Thumbprint SHA-1: | 70B8BA3A50BCDBAD1DC2C86C6DEB1D78215EA111 |
| Thumbprint SHA-256: | 4750C8643DF6099EA03EB3ADA1157EEFC149A3BAC6DBB31760A4DC0AFC41C007 |
| Serial: | 61C3329855F6476CFCB4FCF359E55909 |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x7722 | 0x8000 | False | 0.566650390625 | COM executable for DOS | 6.39486324672 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x9000 | 0xc32 | 0x1000 | False | 0.376708984375 | data | 4.52160108025 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xa000 | 0x410c | 0x3000 | False | 0.0714518229167 | data | 0.996089583315 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xf000 | 0xa20 | 0x1000 | False | 0.26318359375 | data | 4.15843705735 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

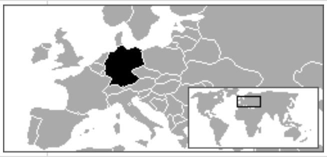
### Imports

### Exports

### Version Infos

### Possible Origin

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

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| English | United States | |
| German | Germany |  |
| French | France | |
| Japanese | Japan | |

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

## System Behavior

### Analysis Process: niPie.exe PID: 6404 Parent PID: 5668

#### General

| | |
|---|---|
| Start time: | 08:37:56 |
| Start date: | 14/10/2021 |
| Path: | C:\Users\user\Desktop\niPie.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\niPie.exe' |
| Imagebase: | 0x400000 |
| File size: | 73664 bytes |
| MD5 hash: | 601FDA01EFB1A22E18A19793158B51FE |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Disassembly

## Code Analysis

---

Joe Sandbox Cloud Basic 33.0.0 White Diamond