
**ID:** 345244
**Sample Name:** fnp_my.dll
**Cookbook:** default.jbs
**Time:** 21:40:13
**Date:** 27/01/2021
**Version:** 31.0.0 Emerald

# Table of Contents

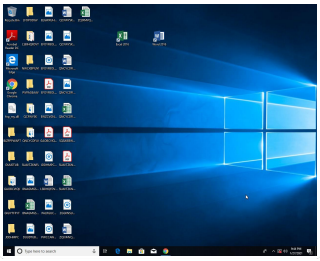
# Analysis Report fnp_my.dll

## Overview

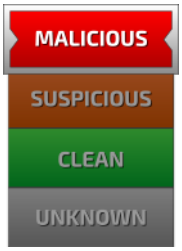
### General Information

| | |
|---|---|
| Sample Name: | fnp_my.dll |
| Analysis ID: | 345244 |
| MD5: | 9e7f0e102da06fe.. |
| SHA1: | 18bf04d09683aa5. |
| SHA256: | 8126a938b442f7f.. |

Most interesting Screenshot:



### Detection

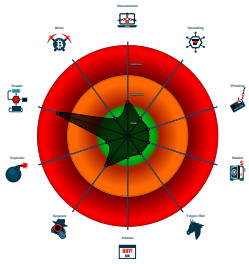



| | |
|---|---|
| Score: | 80 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Hides threads from debuggers
- Machine Learning detection for samp…
- PE file contains section with special…
- Tries to detect sandboxes / dynamic…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Antivirus or Machine Learning detec…
- Checks for debuggers (devices)
- Checks if the current process is bein…
- Contains capabilities to detect virtua…

### Classification



## Startup

- **System is w10x64**
- loaddll32.exe (PID: 6540 cmdline: loaddll32.exe 'C:\Users\user\Desktop\fnp_my.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - rundll32.exe (PID: 6780 cmdline: rundll32.exe C:\Users\user\Desktop\fnp_my.dll,TMethodImplementationIntercept MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6924 cmdline: rundll32.exe C:\Users\user\Desktop\fnp_my.dll,__dbk_fcall_wrapper MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7056 cmdline: rundll32.exe C:\Users\user\Desktop\fnp_my.dll,dbkFCallWrapperAddr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

## Malware Configuration

**No configs have been found**

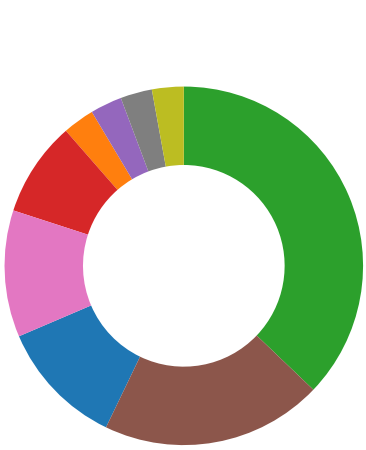
## Yara Overview

**No yara matches**

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview




Click to jump to signature section

## AV Detection:

**Antivirus / Scanner detection for submitted sample**

**Multi AV Scanner detection for submitted file**

**Machine Learning detection for sample**

## Compliance:

**Uses 32bit PE files**

## System Summary:

**PE file contains section with special chars**

## Malware Analysis System Evasion:

**Tries to detect sandboxes / dynamic malware analysis system (registry check)**

**Tries to detect virtualization through RDTSC time measurements**

## Anti Debugging:

**Hides threads from debuggers**

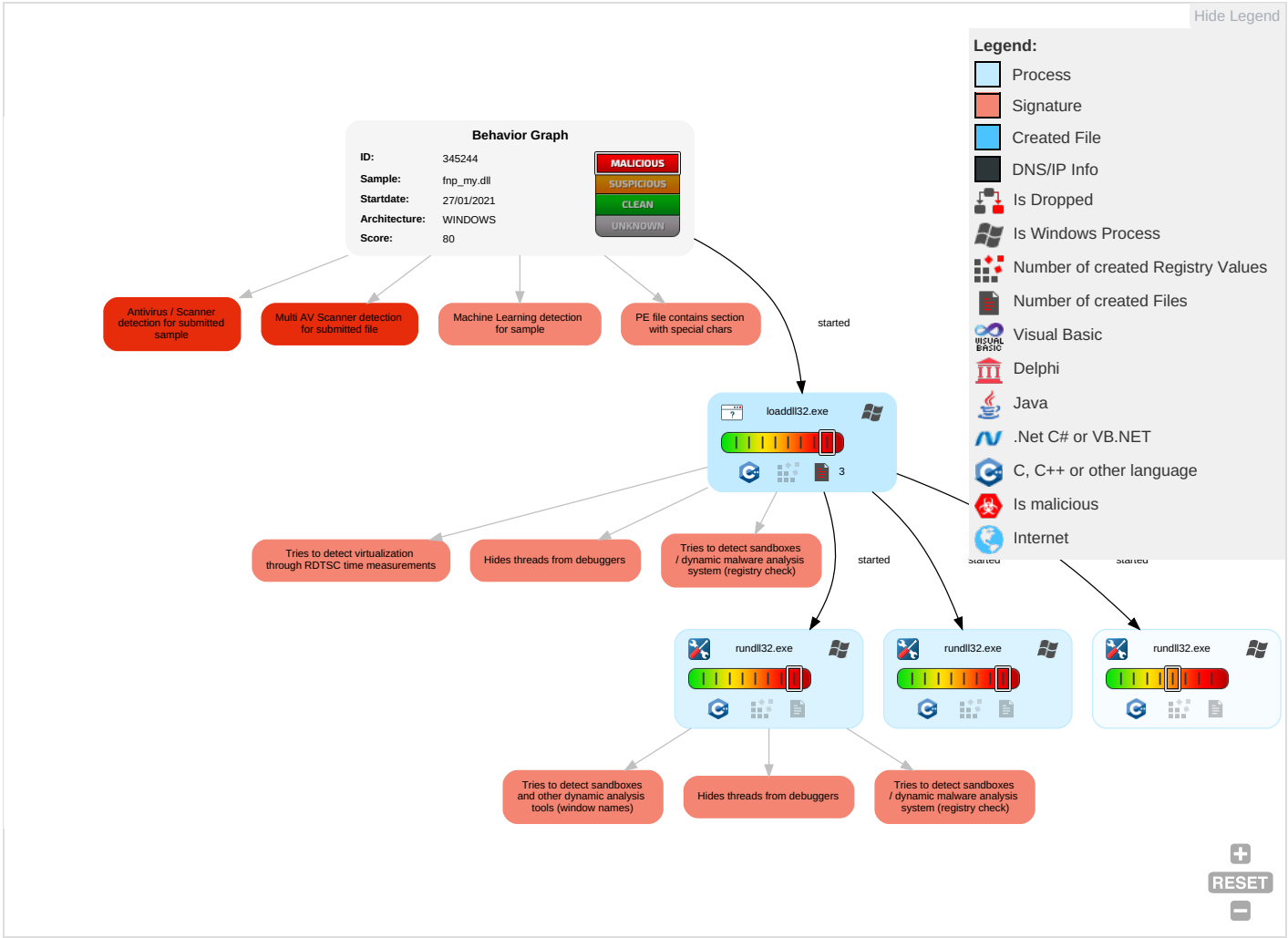
**Tries to detect sandboxes and other dynamic analysis tools (window names)**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 2 | Virtualization/Sandbox Evasion 2 4 | OS Credential Dumping | Security Software Discovery 4 4 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | R T W A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rundll32 1 | LSASS Memory | Virtualization/Sandbox Evasion 2 4 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | R W W A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Software Packing 3 | Security Account Manager | Process Discovery 2 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | O D C B |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 2 | NTDS | System Information Discovery 1 2 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 1 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |

## 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 |
|---|---|---|---|---|
| fnp_my.dll | 34% | Virustotal | | Browse |
| fnp_my.dll | 45% | ReversingLabs | Win32.Trojan.Generic | |
| fnp_my.dll | 100% | Avira | TR/Crypt.TPM.Gen | |
| fnp_my.dll | 100% | Joe Sandbox ML | | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.1.loaddll32.exe.ea0000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 3.2.rundll32.exe.4a10000.1.unpack | 100% | Avira | TR/Crypt.TPM.Gen | | Download File |
| 0.1.loaddll32.exe.ea0000.2.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 3.1.rundll32.exe.4a10000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 0.1.loaddll32.exe.ea0000.3.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 2.1.rundll32.exe.4c90000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 4.1.rundll32.exe.4dd0000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 4.1.rundll32.exe.4dd0000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 0.1.loaddll32.exe.ea0000.1.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 2.1.rundll32.exe.4c90000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |
| 3.1.rundll32.exe.4a10000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen2 | | Download File |

### Domains

**No Antivirus matches**

### URLs

**No Antivirus matches**

## Domains and IPs

### Contacted Domains

**No contacted domains info**

### Contacted IPs

**No contacted IP infos**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Emerald |
| Analysis ID: | 345244 |
| Start date: | 27.01.2021 |
| Start time: | 21:40:13 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 43s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | fnp_my.dll |
| 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: | 28 |
| 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: | mal80.evad.winDLL@7/2@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 60% (good quality ratio 40%)<br>• Quality average: 66.7%<br>• Quality standard deviation: 47.1% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .dll |

| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe<br>• Execution Graph export aborted for target rundll32.exe, PID 6924 because there are no executed function |
|---|---|

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 21:41:15 | API Interceptor | 1x Sleep call for process: loaddll32.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:\ProgramData\mntemp | |
|---|---|
| Process: | C:\Windows\System32\loaddll32.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 16 |
| Entropy (8bit): | 3.75 |
| Encrypted: | false |
| SSDEEP: | 3:V6Z8/5e5:V6Z8xe5 |
| MD5: | 57AE9F6FE8C726D74E5C00A47AE7F4F9 |
| SHA1: | 9888E86DB368FC7A8FCFF4D87F39EDE6144965B6 |
| SHA-256: | D751C19D3C832BB006ED0D3BFB9833715B0DA9523D4661E830B81674A79322A4 |
| SHA-512: | E030417D8B58CADD979390AA7ACD484EFF19A0A67825DCB9E69542556E9BE51F3A1DAF8987CB7F2891F89F7BB51911C056CFEDBB05376887ED576D9E179600DC |
| Malicious: | false |
| Reputation: | low |

| C:\ProgramData\mntemp | |
|---|---|
| Preview: | .P...{:qZ.:..u. |

| C:\ProgramData\yysrkymy.zki | |
|---|---|
| Process: | C:\Windows\System32\loaddll32.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5107 |
| Entropy (8bit): | 7.019361392364344 |
| Encrypted: | false |
| SSDEEP: | 96:61fsqP9p6/PzlTWqcXwpy8JkPR+4rfQPEI9DWkz9+irfa+cZ8CdGDncL:gfT9pYpUwpt+0EuRrCdTdG7i |
| MD5: | 6F668C190D44BE0D06FCB36F647BC5C1 |
| SHA1: | ED70C2CB35FBE77C0864348A8E24127490F4C861 |
| SHA-256: | 3ED8A75FB650DE94D49F26B46CEE76BC2ECBF5ACFDA4EA655854E4FEEA272FE5 |
| SHA-512: | 6E9A4414666F3C9C16B17C56AC85B2DCDFDCCAD48EDE2409CFCFCCE1F5FA7EA434CBE2A004847462EEC2AE20FDF4DFAA29836C899240C00CB36374BF7FB9985 |
| Malicious: | false |
| Reputation: | low |
| Preview: | m.B.S.(j..L...L.....L.m.B.....Q.B.....$.4$.4$...:.!....M.....).[R_..$...G....c...[.....:.c...h`t.^..$.*.....,$.'...TZ.....h!.6..,$...._..w..l....\.....[..$.....,$.....4$.....,$T.,$.....Q.....Y.....U.t$.]..$\U..${.Th..$Sh..}[1\$...$.....YW.2...E../..m.....M.....$\.a....t$..6.....].l...h.$<6..$h.49J..$..?_..../.....Q.....^.....$....\.;.....,$..?.h)l$..J.....?.hS.....R."..O)..4$.N.....4$S.4$.....$....U.4$h.\|p^.2...].4$..$U.....,$\R.c...Z...V.....).^.....^1._.%...U.....]....$.....P.4$..$=.....,$....$$..$.[R.....Z.....3.$1.$3.$\h.-....$.....4$..$R..$...y.....$.....Y.m.....$R..$..o_..$.....4$.....(.Y..[.....,$\.%.....$....\C.7.....)L$.Q..u.k.l$....~.l$..\|./)L$..D$..\|./.D$.. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.928840734574505 |
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.40%<br>• Win16/32 Executable Delphi generic (2074/23) 0.21%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | fnp_my.dll |
| File size: | 5310464 |
| MD5: | 9e7f0e102da06fea22b2f42c7023f4d0 |
| SHA1: | 18bf04d09683aa5c664e0ccf52ac205a974ed9cd |
| SHA256: | 8126a938b442f7fb4d8a405efb6db33890c1b34f8a886bbf764bb618eafe392d |
| SHA512: | 886e876c7f4e8fc301ea67a9cf1c586f28e4f49034e5184e460fe5705bcf0236fed35e5b9192ca66e9e3878aa818bdad0912b251086bfe8096c849347d7a402d |
| SSDEEP: | 98304:OOtTQA8r4xSDJupAk0kcXvJQvkVtcNTOp/6syMB3WB4vCMG0AfyiJwQC:OCDSeZmjqvy1/6tMF5Zb5 |
| File Content Preview: | MZP.....@.....!..L.!..This program must be run under Win32..$7..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0xfc4000 |
| Entrypoint Section: | pdnzzolr |
| Digitally signed: | false |

## General

| | |
|---|---|
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI |
| DLL Characteristics: | |
| Time Stamp: | 0x590341E6 [Fri Apr 28 13:21:42 2017 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 0 |
| File Version Major: | 5 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 0 |
| Import Hash: | baa93d47220682c04d92f7797d9224ce |

## Entrypoint Preview

| Instruction |
|---|
| push esi |
| push eax |
| push ebx |
| call 00007F20E4F7D636h |
| int3 |
| pop eax |
| mov ebx, eax |
| inc eax |
| sub eax, 004A8000h |
| sub eax, 06BF6C28h |
| add eax, 06BF6C1Fh |
| cmp byte ptr [ebx], FFFFFFCCh |
| jne 00007F20E4F7D64Bh |
| mov byte ptr [ebx], 00000000h |
| mov ebx, 00001000h |
| push 192D467Fh |
| push 20C281D5h |
| push ebx |
| push eax |
| call 00007F20E4F7D63Fh |
| add eax, 00000000h |
| mov dword ptr [esp+08h], eax |
| pop ebx |
| pop eax |
| ret |
| push ebp |
| mov ebp, esp |
| push eax |
| push ebx |
| push ecx |
| push esi |
| mov esi, dword ptr [ebp+08h] |
| mov ecx, dword ptr [ebp+0Ch] |
| shr ecx, 02h |
| mov eax, dword ptr [ebp+10h] |
| mov ebx, dword ptr [ebp+14h] |
| test ecx, ecx |
| je 00007F20E4F7D63Ch |
| xor dword ptr [esi], eax |
| add dword ptr [esi], ebx |
| add esi, 04h |
| dec ecx |
| jmp 00007F20E4F7D624h |
| pop esi |
| pop ecx |
| pop ebx |

| Instruction |
|---|
| pop eax |
| leave |
| retn 0010h |
| fidiv word ptr [edi+edx*2+6Ah] |
| cmc |
| adc eax, 7114A3A2h |
| xchg eax, ebx |
| pop esp |
| mov cl, ah |
| inc ebx |
| add byte ptr [edi], ch |
| add eax, 7DDA218Fh |
| dec ebx |
| push ebp |
| jmp 00007F20E4F7D5D0h |
| xchg eax, edx |
| pop es |
| add ebp, dword ptr [eax+edi*4] |
| adc eax, 676B1FEFh |
| sbb al, byte ptr [ebp+12h] |
| cmp al, byte ptr [edi+6B5A17ACh] |
| jc 00007F20E4F7D69Ah |
| inc dword ptr [ebx+46h] |
| sub bl, byte ptr [esi-7Fh] |
| out dx, al |
| retn FF92h |
| xchg byte ptr [eax-48h], ch |
| or eax, dword ptr [eax] |
| add byte ptr [ecx+12682434h], cl |
| pop ds |
| add byte ptr [eax], al |
| mov dword ptr [esp], eax |
| mov ebx, 678C1325h |
| mov eax, D1643A86h |
| sub eax, ebx |
| add ebx, 00000000h |

## Data Directories

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0xbc354c | 0x98 | ipjhmkim |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0x14406d | 0x95 | .idata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0x13f000 | 0x4200 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0x1441f8 | 0x8 | .idata |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x122000 | 0x1ea | |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_RESERVED | 0x0 | 0x0 | |

## Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| | 0x1000 | 0x13e000 | 0x66200 | False | 0.998778400398 | data | 7.98647327711 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .rsrc | 0x13f000 | 0x4200 | 0x1800 | False | 0.833658854167 | data | 7.1537166158 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .idata | 0x144000 | 0x1000 | 0x200 | False | 0.181640625 | data | 1.29348767602 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
|  | 0x145000 | 0x5d7000 | 0x200 | unknown | unknown | unknown | unknown | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| ipjhmkim | 0x71c000 | 0x4a8000 | 0x4a7800 | unknown | unknown | unknown | unknown | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| pdnzzolr | 0xbc4000 | 0x1000 | 0x200 | False | 1.021484375 | data | 7.23203811633 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |

## Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_STRING | 0x13f490 | 0x70 | data |  |  |
| RT_STRING | 0x13f500 | 0x364 | data |  |  |
| RT_STRING | 0x13f864 | 0x398 | data |  |  |
| RT_STRING | 0x13fbfc | 0x334 | MPEG ADTS, layer II, v2,  80 kbps, 16 kHz, Monaural |  |  |
| RT_STRING | 0x13ff30 | 0x478 | data |  |  |
| RT_STRING | 0x1403a8 | 0x350 | data |  |  |
| RT_STRING | 0x1406f8 | 0x3bc | data |  |  |
| RT_STRING | 0x140ab4 | 0x5bc | empty |  |  |
| RT_STRING | 0x141070 | 0x398 | empty |  |  |
| RT_STRING | 0x141408 | 0x448 | empty |  |  |
| RT_STRING | 0x141850 | 0x210 | empty |  |  |
| RT_STRING | 0x141a60 | 0xbc | empty |  |  |
| RT_STRING | 0x141b1c | 0x100 | empty |  |  |
| RT_STRING | 0x141c1c | 0x338 | empty |  |  |
| RT_STRING | 0x141f54 | 0x478 | empty |  |  |
| RT_STRING | 0x1423cc | 0x354 | empty |  |  |
| RT_STRING | 0x142720 | 0x2b8 | empty |  |  |
| RT_RCDATA | 0x1429d8 | 0x10 | empty |  |  |
| RT_RCDATA | 0x1429e8 | 0x4a0 | empty |  |  |
| RT_RCDATA | 0x142e88 | 0x2 | empty | English | United States |
| RT_VERSION | 0xbc35e4 | 0x1f4 | data | English | United States |

## Imports

| DLL | Import |
|---|---|
| kernel32.dll | lstrcpy |
| comctl32.dll | InitCommonControls |

## Exports

| Name | Ordinal | Address |
|---|---|---|
| TMethodImplementationIntercept | 3 | 0x45cfac |
| __dbk_fcall_wrapper | 2 | 0x410388 |
| dbkFCallWrapperAddr | 1 | 0x5195ac |

## Version Infos

| Description | Data |
|---|---|
| ProductName | fnp_my |
| ProgramID | com.embarcadero.fnp_my |
| FileDescription | fnp_my |
| FileVersion | 1.0.0.0 |
| ProductVersion | 1.0.0.0 |
| Translation | 0x0409 0x04e4 |

## Possible Origin

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

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

### Behavior

loaddll32.exe
rundll32.exe
rundll32.exe
rundll32.exe

Click to jump to process

## System Behavior

### Analysis Process: loaddll32.exe PID: 6540 Parent PID: 5812

#### General

| | |
|---|---|
| Start time: | 21:41:00 |
| Start date: | 27/01/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe 'C:\Users\user\Desktop\fnp_my.dll' |
| Imagebase: | 0x380000 |
| File size: | 120832 bytes |
| MD5 hash: | 2D39D4DFDE8F7151723794029AB8A034 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: rundll32.exe PID: 6780 Parent PID: 6540

### General

| | |
|---|---|
| Start time: | 21:41:04 |
| Start date: | 27/01/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\fnp_my.dll,TMethodImplementationIntercept |
| Imagebase: | 0xcb0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

## Analysis Process: rundll32.exe PID: 6924 Parent PID: 6540

### General

| | |
|---|---|
| Start time: | 21:41:08 |
| Start date: | 27/01/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\fnp_my.dll,__dbk_fcall_wrapper |
| Imagebase: | 0xcb0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 7056 Parent PID: 6540

### General

| | |
|---|---|
| Start time: | 21:41:11 |
| Start date: | 27/01/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\fnp_my.dll,dbkFCallWrapperAddr |

| | |
|---|---|
| Imagebase: | 0xcb0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities**

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

# Disassembly

## Code Analysis