
**ID:** 677709
**Sample Name:** pmfoxWgt1q
**Cookbook:** default.jbs
**Time:** 22:11:31
**Date:** 02/08/2022
**Version:** 35.0.0 Citrine

# Table of Contents

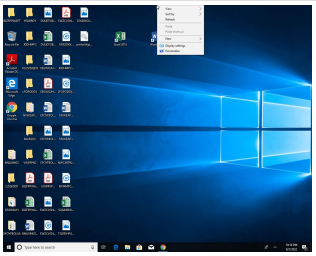
# Windows Analysis Report

## pmfoxWgt1q

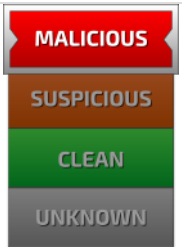
## Overview

### General Information

| | |
|---|---|
| Sample Name: | pmfoxWgt1q (renamed file extension from none to dll) |
| Analysis ID: | 677709 |
| MD5: | 6300568039c3d3.. |
| SHA1: | bef385861ab3ad.. |
| SHA256: | 55d87fda07c855.. |
| Infos: | |



### Detection



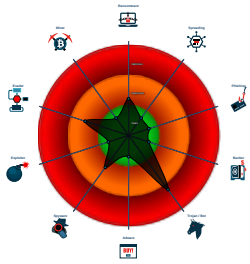

Emotet

| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Multi AV Scanner detection for subm…
- Tries to load missing DLLs
- Contains functionality to check if a d…
- Contains functionality to query local…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Registers a DLL

### Classification



## Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5168 cmdline: loaddll64.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 5176 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5196 cmdline: rundll32.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 5184 cmdline: regsvr32.exe /s C:\Users\user\Desktop\pmfoxWgt1q.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5212 cmdline: rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5316 cmdline: rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,YAeJyEAYL7F4eDck6YUaf MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5332 cmdline: rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,fmFkmnQYB5TC2Sq5NGFkK MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Signatures

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| pmfoxWgt1q.dll | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |

### Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000004.00000002.882940563.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000005.00000002.882553231.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 00000006.00000002.889058366.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 00000002.00000002.881462250.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 00000003.00000002.882940823.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| Click to see the 1 entries | | | | |

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 5.2.rundll32.exe.7ffc739f0000.0.unpack | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 2.2.regsvr32.exe.7ffc739f0000.0.unpack | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 4.2.rundll32.exe.7ffc739f0000.0.unpack | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.7ffc739f0000.0.unpack | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| 0.2.loaddll64.exe.7ffc739f0000.0.unpack | JoeSecurity_Emotet_2 | Yara detected Emotet | Joe Security | |
| Click to see the 1 entries | | | | |

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

## Joe Sandbox Signatures

### AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

### E-Banking Fraud

Yara detected Emotet

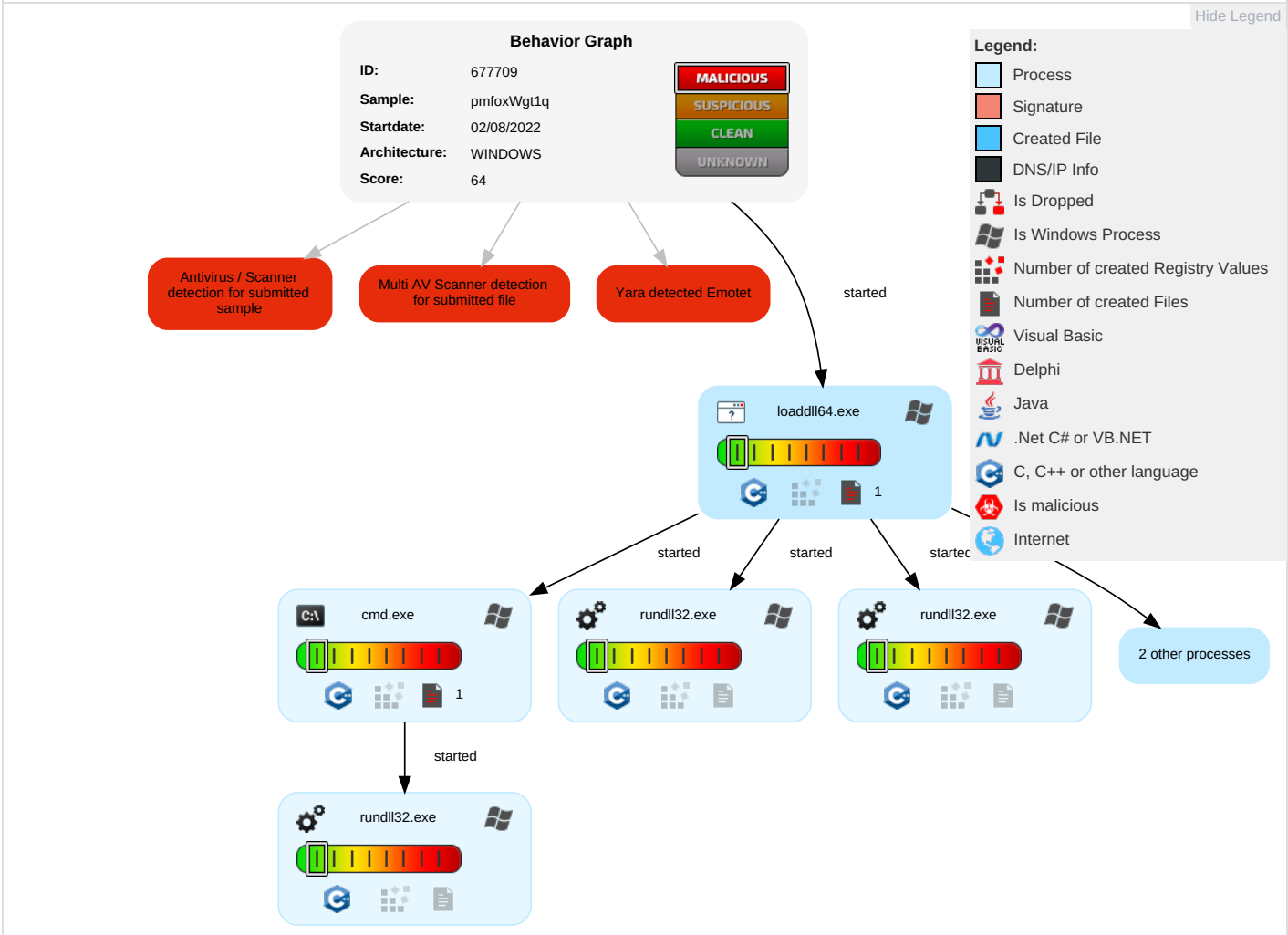
### Stealing of Sensitive Information

Yara detected Emotet

## 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 | Windows Management Instrumentation | 1 DLL Side-Loading | 1 1 Process Injection | 1 Regsvr32 | OS Credential Dumping | 1 System Time Discovery | Remote Services | 1 Archive Collected Data | Exfiltration Over Other Network Medium | 1 Encrypted Channel | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | 1 DLL Side-Loading | 1 Rundll32 | LSASS Memory | 2 Security Software Discovery | 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 |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | 1 1 Process Injection | Security Account Manager | 1 File and Directory Discovery | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delete Device Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | 1 Deobfuscate/Decode Files or Information | NTDS | 2 2 System Information Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carrier Billing Fraud |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | 1 DLL Side-Loading | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | 2 Obfuscated Files or Information | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service | | Abuse Accessibility Features |

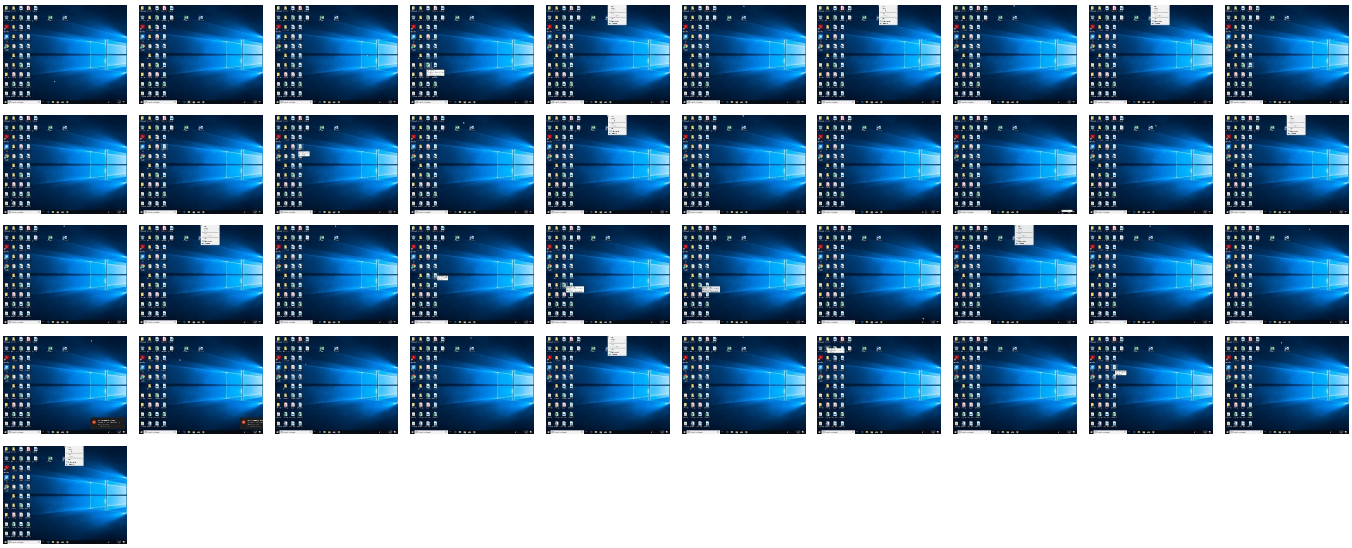
## Behavior Graph



# 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 |
|---|---|---|---|---|
| pmfoxWgt1q.dll | 34% | Metadefender | | Browse |
| pmfoxWgt1q.dll | 72% | ReversingLabs | Win64.Trojan.Emotet | |
| pmfoxWgt1q.dll | 100% | Avira | TR/Kryptik.assob | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## World Map of Contacted IPs

No contacted IP infos

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 35.0.0 Citrine |
| Analysis ID: | 677709 |
| Start date and time: 02/08/202222:11:31 | 2022-08-02 22:11:31 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 15s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | pmfoxWgt1q (renamed file extension from none to 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: | 19 |
| 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: | mal64.troj.winDLL@13/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<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 rundll32 |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- VT rate limit hit for: pmfoxWgt1q.dll

## Simulations

### Behavior and APIs

**No simulations**

## Joe Sandbox View / Context

### IPs

**No context**

### Domains

**No context**

### ASNs

**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 (DLL) (GUI) x86-64, for MS Windows |
| Entropy (8bit): | 6.627867897691371 |
| TrID: | • Win64 Dynamic Link Library (generic) (102004/3) 86.43%<br>• Win64 Executable (generic) (12005/4) 10.17%<br>• Generic Win/DOS Executable (2004/3) 1.70%<br>• DOS Executable Generic (2002/1) 1.70%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01% |
| File name: | pmfoxWgt1q.dll |
| File size: | 866816 |
| MD5: | 6300568039c3d35aaa0fc0f59a6089df |
| SHA1: | bef385861ab3ad1bf5c1c76384ccf45a75c80ed5 |
| SHA256: | 55d87fda07c8550c926974930480cf4899fed628ef544164519984efa447014a |
| SHA512: | 2150699d801fe40d2fb7675799b85220ead4dde32b8fcd3e073b2765657a15259156f4d35b2b3b8386ebe3167e484452162fdb5246230343d7d3096753d0fbc3 |
| SSDEEP: | 24576:sPMTg9U3G0ISDKvSeqfZaePWAy7ympE3:BTg9UXRD2SeqfZZi2m |
| TLSH: | FD05283FD6590A62FC1F1235C642894BF591FA0223145D9EB3AE0A58DF3BE48F9A5F10 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K._]..1...1...1...2...1...4...1...5...1.m.5...1.m.2...1.m.4.I.1...0...1...0.I.1...8...1...1...1.....1.....1...3...1.Rich..1 |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x180073c20 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x180000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL |
| DLL Characteristics: | HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x6284F4EB [Wed May 18 13:30:19 2022 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 5c49ce3660f3f487a221bd7888983b24 |

### Entrypoint Preview

| Instruction |
|---|
| dec eax |
| mov dword ptr [esp+08h], ebx |
| dec eax |
| mov dword ptr [esp+10h], esi |
| push edi |
| dec eax |
| sub esp, 20h |
| dec ecx |
| mov edi, eax |
| mov ebx, edx |
| dec eax |

| Instruction |
| --- |
| mov esi, ecx |
| cmp edx, 01h |
| jne 00007F0EE09B8387h |
| call 00007F0EE09B8B48h |
| dec esp |
| mov eax, edi |
| mov edx, ebx |
| dec eax |
| mov ecx, esi |
| dec eax |
| mov ebx, dword ptr [esp+30h] |
| dec eax |
| mov esi, dword ptr [esp+38h] |
| dec eax |
| add esp, 20h |
| pop edi |
| jmp 00007F0EE09B8214h |
| int3 |
| int3 |
| int3 |
| dec eax |
| sub esp, 28h |
| call 00007F0EE09B8F8Ch |
| test eax, eax |
| je 00007F0EE09B83A3h |
| dec eax |
| mov eax, dword ptr [00000030h] |
| dec eax |
| mov ecx, dword ptr [eax+08h] |
| jmp 00007F0EE09B8387h |
| dec eax |
| cmp ecx, eax |
| je 00007F0EE09B8396h |
| xor eax, eax |
| dec eax |
| cmpxchg dword ptr [000309E4h], ecx |
| jne 00007F0EE09B8370h |
| xor al, al |
| dec eax |
| add esp, 28h |
| ret |
| mov al, 01h |
| jmp 00007F0EE09B8379h |
| int3 |
| int3 |
| int3 |
| dec eax |
| sub esp, 28h |
| call 00007F0EE09B8F50h |
| test eax, eax |
| je 00007F0EE09B8389h |
| call 00007F0EE09B8D9Bh |
| jmp 00007F0EE09B839Bh |
| call 00007F0EE09B65DCh |
| mov ecx, eax |
| call 00007F0EE09C43A1h |
| test eax, eax |
| je 00007F0EE09B8386h |
| xor al, al |

| Instruction |
|---|
| jmp 00007F0EE09B8389h |
| call 00007F0EE09C4760h |
| mov al, 01h |
| dec eax |
| add esp, 28h |
| ret |
| dec eax |
| sub esp, 28h |
| xor ecx, ecx |
| call 00007F0EE09B84C2h |
| test al, al |
| setne al |
| dec eax |
| add esp, 28h |
| ret |
| int3 |
| int3 |

**Data Directories**

| Name | Virtual Address | Virtual Size | Is in Section |
|---|---|---|---|
| IMAGE_DIRECTORY_ENTRY_EXPORT | 0xa1de0 | 0xb0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_IMPORT | 0xa1e90 | 0x3c | .rdata |
| IMAGE_DIRECTORY_ENTRY_RESOURCE | 0xa9000 | 0x2ea20 | .rsrc |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION | 0xa6000 | 0x1fe0 | .pdata |
| IMAGE_DIRECTORY_ENTRY_SECURITY | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_BASERELOC | 0xd8000 | 0x914 | .reloc |
| IMAGE_DIRECTORY_ENTRY_DEBUG | 0x9e6e0 | 0x38 | .rdata |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_TLS | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG | 0x9e5a0 | 0x140 | .rdata |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT | 0x0 | 0x0 | |
| IMAGE_DIRECTORY_ENTRY_IAT | 0x91000 | 0x2c0 | .rdata |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT | 0x0 | 0x0 | |
| 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 |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x8f260 | 0x8f400 | False | 0.3861392888307155 | data | 6.011164043310419 | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ |
| .rdata | 0x91000 | 0x117ce | 0x11800 | False | 0.4552734375 | data | 5.141486524366641 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0xa3000 | 0x2940 | 0x1200 | False | 0.17078993055555555 | DOS executable (block device driver) | 2.811233564125507 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .pdata | 0xa6000 | 0x1fe0 | 0x2000 | False | 0.48046875 | data | 5.507319499503956 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| _RDATA | 0xa8000 | 0x15c | 0x200 | False | 0.40625 | data | 3.363296824709797 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .rsrc | 0xa9000 | 0x2ea20 | 0x2ec00 | False | 0.8596361129679144 | data | 7.814152582292596 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xd8000 | 0x914 | 0xa00 | False | 0.4828125 | data | 5.246908112940421 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

| Name | RVA | Size | Type | Language | Country |
|---|---|---|---|---|---|
| RT_FONTDIR | 0xa90a0 | 0x2e800 | data | English | United States |
| RT_MANIFEST | 0xd78a0 | 0x17d | XML 1.0 document text | English | United States |

### Imports

| DLL | Import |
|---|---|
| ole32.dll | CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc |
| KERNEL32.dll | ExitProcess, WriteConsoleW, CreateFileW, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, EncodePointer, DecodePointer, MultiByteToWideChar, WideCharToMultiByte, LCMapStringEx, GetStringTypeW, GetCPInfo, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, RtlUnwindEx, RtlPcToFileHeader, RaiseException, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, RtlUnwind, GetModuleHandleExW, GetModuleFileNameW, HeapFree, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, HeapAlloc, GetStdHandle, GetFileType, CloseHandle, FlushFileBuffers, WriteFile, GetConsoleOutputCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, ReadConsoleW, HeapReAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetProcessHeap, SetStdHandle, HeapSize |

### Exports

| Name | Ordinal | Address |
|---|---|---|
| DllRegisterServer | 1 | 0x180070020 |
| YAeJyEAYL7F4eDck6YUaf | 2 | 0x1800702c0 |
| fmFkmnQYB5TC2Sq5NGFkK | 3 | 0x1800701e0 |
| nrDjhnkd9nedaQwcCY | 4 | 0x180070100 |

### Possible Origin

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

## Network Behavior

No network behavior found

## Statistics

### Behavior

- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe

Click to jump to process

# System Behavior

## Analysis Process: loaddll64.exe PID: **5168**, Parent PID: **616**

| General | |
|---|---|
| Target ID: | 0 |
| Start time: | 22:12:36 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\loaddll64.exe |
| Wow64 process (32bit): | false |
| Commandline: | loaddll64.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll" |
| Imagebase: | 0x7ff66a740000 |
| File size: | 140288 bytes |
| MD5 hash: | 4E8A40CAD6CCC047914E3A7830A2D8AA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000000.00000002.880853299.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

## Analysis Process: cmd.exe PID: **5176**, Parent PID: **5168**

| General | |
|---|---|
| Target ID: | 1 |
| Start time: | 22:12:36 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\cmd.exe |
| Wow64 process (32bit): | false |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll",#1 |
| Imagebase: | 0x7ff6499e0000 |
| File size: | 273920 bytes |
| MD5 hash: | 4E2ACF4F8A396486AB4268C94A6A245F |
| Has elevated privileges: | true |

| | |
|---|---|
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

| File Activities | | | | | | | |
|---|---|---|---|---|---|---|---|
| There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it. | | | | | | | |
| **File Path** | **Access** | **Attributes** | **Options** | **Completion** | **Count** | **Source Address** | **Symbol** |

## Analysis Process: regsvr32.exe PID: **5184**, Parent PID: **5168**

### General

| | |
|---|---|
| Target ID: | 2 |
| Start time: | 22:12:37 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | regsvr32.exe /s C:\Users\user\Desktop\pmfoxWgt1q.dll |
| Imagebase: | 0x7ff619650000 |
| File size: | 24064 bytes |
| MD5 hash: | D78B75FC68247E8A63ACBA846182740E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000002.00000002.881462250.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5196**, Parent PID: **5176**

### General

| | |
|---|---|
| Target ID: | 3 |
| Start time: | 22:12:37 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\pmfoxWgt1q.dll",#1 |
| Imagebase: | 0x7ff6dbdb0000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000003.00000002.882940823.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5212**, Parent PID: **5168**

### General

| | |
|---|---|
| Target ID: | 4 |
| Start time: | 22:12:37 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,DllRegisterServer |

| | |
|---|---|
| Imagebase: | 0x7ff6dbdb0000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000004.00000002.882940563.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5316**, Parent PID: **5168**

### General

| | |
|---|---|
| Target ID: | 5 |
| Start time: | 22:12:41 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,YAeJyEAYL7F4eDck6YUaf |
| Imagebase: | 0x7ff6dbdb0000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000005.00000002.882553231.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: **5332**, Parent PID: **5168**

### General

| | |
|---|---|
| Target ID: | 6 |
| Start time: | 22:12:45 |
| Start date: | 02/08/2022 |
| Path: | C:\Windows\System32\rundll32.exe |
| Wow64 process (32bit): | false |
| Commandline: | rundll32.exe C:\Users\user\Desktop\pmfoxWgt1q.dll,fmFkmnQYB5TC2Sq5NGFkK |
| Imagebase: | 0x7ff6dbdb0000 |
| File size: | 69632 bytes |
| MD5 hash: | 73C519F050C20580F8A62C849D49215A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_2, Description: Yara detected Emotet, Source: 00000006.00000002.889058366.00007FFC739F1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security |
| Reputation: | high |

# Disassembly

**No disassembly**