# Analysis of a DLL Downloader

cyberandramen.net/2022/01/23/analysis-of-a-dll-downloader/

January 23, 2022

## Summary

SHA256: dedb8516befa4a5088000b8c7f699dae7f33761403dd355a14684ac89ff56a9a

- Filename: Unknown
- Filetype: DLL
- File size: 39KB

From here on, the above DLL will be referred to as “downloader.dll”. The file is capable of:

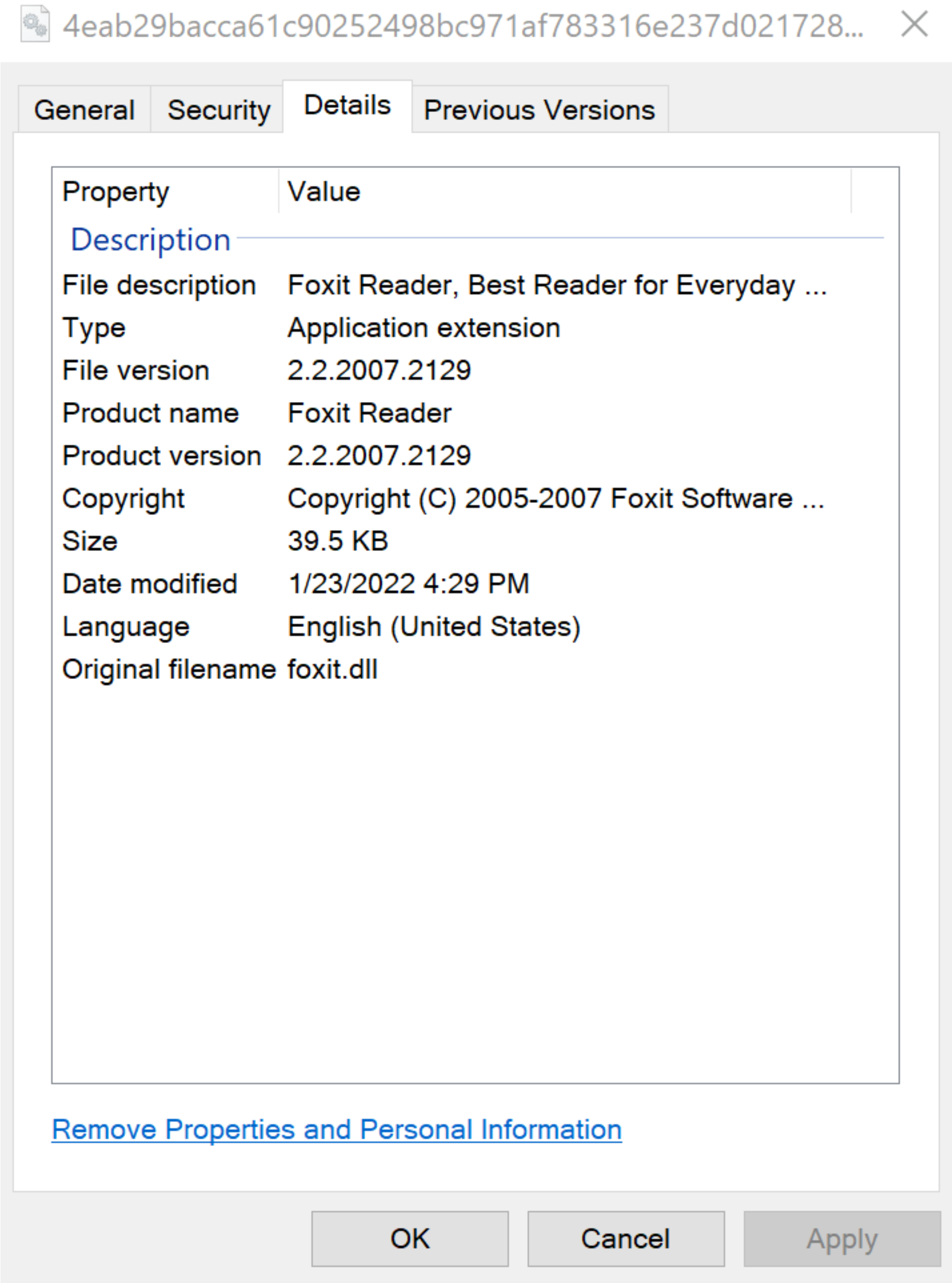
- Downloading files
- Interacting with a C2 server

## Malware Overview

This is an older file that was first identified around October 2021.

Downloader.dll is a downloader capable of downloading a file from a hardcoded command and control (C2) server. A follow-on stage was not identified.

The file disguises itself as an extension for Foxit Reader software. Foxit is a software that develops document formatting tools and is based in the U.S. and China.



4eab29bacca61c90252498bc971af783316e237d021728...
General
Security
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

| Property | Value |
|---|---|
| **Description** | |
| File description | Foxit Reader, Best Reader for Everyday ... |
| Type | Application extension |
| File version | 2.2.2007.2129 |
| Product name | Foxit Reader |
| Product version | 2.2.2007.2129 |
| Copyright | Copyright (C) 2005-2007 Foxit Software ... |
| Size | 39.5 KB |
| Date modified | 1/23/2022 4:29 PM |
| Language | English (United States) |
| Original filename | foxit.dll |

Figure 1

Upon running the DLL, a request is made to online-manual.c1[.]biz, and a file is downloaded to %TEMP%. Looking at the strings output of the file, there is a large base64 encoded string that when decoded, appears to be a batch file as seen below.

```
@echo off

cd /d %TEMP%
:WAITING
timeout /t 1
if not exist "a.log" (goto WAITING)
del /f /q "a.log"
install.bat
del /f /q "%~dpnx0"
```

Again analyzing just the strings, we see a call to run the batch file via the following command:

```
cmd /c cd /d "%TEMP%" && temp.bat
```

One can only assume that the downloaded file is run with another command run via the DLL file:

```
cmd /c expand "%s" -F:* "%s" && del /f /q "%s" && echo OK > a.log
```

The encoded strings represented by “%s” are likely the downloaded file. We can see from the above output that the file is deleted upon the above command completing.

## Network Indicators

- online-manual.c1[.]biz
- http://online-manual.c1%5B.%5Dbiz/index.php?user_id=765&type=

The above infrastructure was tied to a possible Konni campaign by Black Lotus Labs in late November 2021.

> Looks similar to this prior campaign from about a month ago
> SHA1: 9e6ac79b8eaaa01e7aefe7c896de0944e298549d
> SHA1: 9654e17a2b9fe027b5de3c184fac85248887a9ba
> SHA1: 518a35bf8c16d5c5c45053c4bdb548529d4b4d74
> C2:hxxp://online-manual[.]c1[.]biz
>
> — Black Lotus Labs (@BlackLotusLabs) November 19, 2021

## Strings

- online-manual.c1.biz
- cmd /c expand “%s” -F:* “%s” && del /f /q “%s” && echo OK > a.log
- /index.php?user_id=765&type=%d
- \temp.bat
- cmd / c cd /d “%TEMP%” && temp.bat
- QGVjaG8gb2ZmDQoNCmNkIC9kICVURU1QJQ0KOldBSVRJTkcNCnRpbWVvdXQgL3QgMQ0KaWYgbm90IGV4aXN0ICJhLmxvZyIgKGdvd

## Basic Snort/Suricata Rule

alert tcp $HOME_NET any -> any any (msg: “Probaly shouldnt run in production. Possible Konni DLL download URL,”; content: “index.php/user_id=”; content:”&type=”; threshold:type limit, track by_src, count 1, seconds m; sid:999999

Unfortunately, the C2 is likely no longer active, and this sample crashes when run in a sandbox. Still, this is an interesting sample that is likely tied to Konni, and learning occurred, so that is always a win!

Thank you for reading.