Trojan-as-a-service: From Formbook to XLoader

Archived: 2026-04-06 00:53:19 UTC

Summary

- Name: XLoader
- First discovered in October 2020
- Works as malware-as-a-service
- Distributed using spam emails as an email attachment and through vulnerable servers
- Targets Windows and macOS machinesPayload can record keystrokes, take screenshots and obtain info stored on the clipboard. It also steals usernames and passwords from browsers, messengers and email clients.
- Written in C and Assembler
- 32-bit samples, zipped in various file types

Introduction

Discovered in 2016, Formbook appeared on underground forums, advertised as an infostealer for Windows. In October 2020, Formbook was renamed XLoader; as its developers say, it has the same features, but has improved from the previous version. Written in C and Assembler, the malware can steal users' information from various browsers, email clients and messengers. The developers offer malware-as-a-service for $59 per month for the Windows version and $49 for the macOS version.

On October 23, 2020, Formbook malware was rebranded and is now called XLoader, while possessing the same payload as before. On July 21, 2021, the community was informed about the new macOS version.

Technical details

Delivery

As mentioned before, the backdoor is spread with spam emails as an email attachment. It can be single or multiple files camouflaged as archive files (.iso, .rar), pictures, or text files.

EXE disguised as ISO

Above you can see the .iso — an optical disc image file that can be opened with any archiver. Although the file icon picture looks like a standard Microsoft Excel file (.xlsx), this file is a 32-bit executable without any digital signatures (SHA256:8D20C36D499A614206967F9FFE68885A78AA2E7C718512A31B185BBAA529A4F6).

The file manifest contains supported OS ID, which tells that the program has compatibility with *Windows 7* and *Windows Vista*.

The executable file is an installer, created with the Nullsoft Scriptable Installation System (NSIS). During execution, an installer obtains access to the %Temp% folder where it creates its own folder, dropping a DLL there. It will use this file for further operations. This whole process is invisible to the victim.

During execution, the trojan will write some information to the one of dropped files, whose content is encoded in UTF-16 LE format. Also, XLoader adds a reference to itself to the Windows registry at *HKLM\System\CurrentControlSet\bam\State\UserSettings* to enable autostart.

The full process tree captured with *procdot* utility:

EXE disguised as RAR archive

XLoader can be also delivered as a RAR archive, which contains only one file — a 32-bit executable (SHA256:3E23BF4937349C5F5CF233E30658562FCA94D58790EBBE693E176FB595FB0B34). Looking at the PE manifest, the supported OSs are Windows 7 and Windows Vista.

As with the previous file, this one is also an installer, created with NSIS. But in this case, it creates two folders, dropping two DLLs and two files without any extensions. During execution, the malware will also write information in these two files in an ANSI format.

The full process tree, captured with *procdot* utility:

File name

SHA256

Description

xvrlmglvtnb.dll

EFE3E128AE092CA256430703134726A18A1E033D17743699FAFDA97116B3AA0F

Trojan-Injector

rove.exe

3E23BF4937349C5F5CF233E30658562FCA94D58790EBBE693E176FB595FB0B34

Trojan-Dropper

xijmiin

63B9DEFD2CC26656AEA4E223ED58280A411DD8FB56AF9F2810ABC27AB0897C43

data

System.dll

DC58D8AD81CACB0C1ED72E33BFF8F23EA40B5252B5BB55D393A0903E6819AE2F

Memory management DLL

jml6b7kq4g0oolfd

2AA973EADA8988FAAEF087616AB1F56697E1453190CBBF3F4A1338D92B6F30A0

data

Decoy XLSX file that executes VBS

XLoader can be also delivered in a spear-phishing email as an .xlsx file format, which is a spreadsheet created in Microsoft Excel. The file is password-protected and contains a decoy picture with information stating that "the document is protected" and forces a user to "Enable Editing" to execute a Visual Basic script.

MS Excel starts the Microsoft equation editor (EQNEDT32.exe) as a COM object and uses it to execute 'C:\Users\Public\vbc.exe' exploiting the CVE-2017-11882 vulnerability. On behalf of the *EQNEDT32.exe* process, the trojan will establish a connection to the server and retrieve the file (*cc200.exe*) from the following destination:

hxxp://vibexonly.ddns[.]net/taiwan/cc200.exe
SHA256: 146f5b2544e98818cbe9813068d6f08037df0e29a3b83d4d2fce3e1bfc444f2a
Original file name: VectorToListAdapter.exe

Payload

Once executed, the downloaded version of XLoader (*cc200.exe*) performs the following operations:

- Checks supported languages
- Reads the computer and user names
- Checks for the presence of debuggers and sandboxes
- Obtains system information
- Decrypts malicious DLL files from resources and uses them
- Injects PE file into foreign processes
- Collects information for stealing
- Connects to the C&C server through explorer.exe

The downloaded file is a 32-bit executable written in Visual Basic. It contains multiple resources, and also a file description which includes a false company name (Parklane Hosiery), file version and the original file name *VectorToListAdapter.exe.*

Hosiery.ExtendedLinguisticServices contains methods for determining user language and uses InteropTools for viewing and editing the device registry, certificates, application and device info.

The *WebServices* class, located in *Hosiery.My.MyProject(),* has functions for establishing connections to the internet and uses a SOAP HTTP protocol for exchanging messages. Malware uses the system process *explorer.exe* to connect to the C&C servers.

During execution, XLoader decrypts three more libraries from the image resource, using steganography techniques.

One of the libraries contains a *Fedree()* method with a function to decrypt the resource inside. Once the resource is loaded, it passes through the *XOR_DEC* function with a key. After the resource is decrypted, the *Unscramble()* function uses it to form the final payload.

After the decryption routine is ended, the result will be given to the *StartInject()* function, which will proceed with the injection process.

C&C communication

Instead of connecting to C&C servers by itself, XLoader uses one of the system processes; for example, *explorer.exe*. XLoader then uses the process injection technique *(Mitre Att&ck ID: T1055.012 - Process Injection: Process Hollowing)*. To do that, it starts the process in suspended mode using *CreateProcess()*, unmaps the process with *NtUnmapViewOfSection()* from *ntdll.dll*, writes malicious code to the process using *WriteProcessMemory()* and resumes the process. After XLoader successfully injects the process, it deletes its original executable file (rove.exe). The infected process starts execution of malicious code, which includes:

- Choosing one of domains from the list
- Generating fake and real C&C domains
- Providing a connection to the server
- Exchanging messages

Obfuscation

XLoader uses WinAPI call obfuscation. Instead of function names, their hash values are used, which makes the malicious code more difficult to analyze and detect.

DLL files, which are decrypted during execution from the downloaded .NET file, have very obfuscated function names and variable values.

Network activity

As mentioned before, XLoader connects to the C&C servers through the altered *explorer.exe* process. Injected malicious code randomly chooses 16 of 64 domains to search for servers and connects them. During the analysis, XLoader (cc200.exe) tried to establish a connection to the following C&C servers:

- hxxp://www.ethanmillsom.com/
- hxxp://www.vectoroutlines.com/
- hxxp://www.adultpeace.com/
- hxxp://www.sonderbach.net/
- hxxp://www.bigplatesmallwallet.com/
- hxxp://www.alfenas.info/
- hxxp://www.newmopeds.com/
- hxxp://www.boogerstv.com/

- hxxp://www.dmgt4m2g8y2uh.net/
- hxxp://www.aideliveryrobot.com/
- hxxp://www.cyrilgraze.com/
- hxxp://www.brunoecatarina.com/
- hxxp://www.ololmychartlogin.com/
- hxxp://www.malcorinmobiliaria.com/
- hxxp://www.fuhaitongxin.com/

Detected by Acronis

XLoader components are successfully detected by Acronis Cyber Protect.

Conclusion

XLoader is a botnet that evolved from the Formbook infostealer and promotes malware-as-a-service for Windows and macOS. This malware spreads via email attachments and its files can have normal-looking extensions with malicious code, which will be automatically executed when the victim opens the file. Some files are created with the NSIS system and are installers that can drop more files.

Although all files have functions to create windows, they do not appear on the user's screen and all processes are invisible. Malicious code also has obfuscated WinAPI functions, which makes it harder to analyze. The malware doesn’t have hardcoded IPs for command-and-control servers and provides a connection to the servers via other system processes.

IoCs

Files

File name

SHA256

BERN210819.iso

1ea2c02f87744c96ef37390bbc851ddffde8cf691356a07810e590056acf7556

BERN210819.exe

8D20C36D499A614206967F9FFE68885A78AA2E7C718512A31B185BBAA529A4F6

sbsuivaaf4

40183F1A4E282A6BC4239EE44DA42D0BB36B882C10B2C10085BA27294D1D0C02

xvrlmglvtnb.dll

EFE3E128AE092CA256430703134726A18A1E033D17743699FAFDA97116B3AA0F

New P.O From customer.rar

75b93f2e697b637978a15ebaa52fb3f2f325764b2dfef2f254bfba4caa2064b1

rove.exe

3E23BF4937349C5F5CF233E30658562FCA94D58790EBBE693E176FB595FB0B34

xijmiin

63B9DEFD2CC26656AEA4E223ED58280A411DD8FB56AF9F2810ABC27AB0897C43

System.dll

DC58D8AD81CACB0C1ED72E33BFF8F23EA40B5252B5BB55D393A0903E6819AE2F

jml6b7kq4g0oolfd

2AA973EADA8988FAAEF087616AB1F56697E1453190CBBF3F4A1338D92B6F30A0

CONTRACT.xlsx

33ab3e8b6b9e120f172452af47ef4478cac25fac68982451ea0d5a773bae5488

cc200.exe

146F5B2544E98818CBE9813068D6F08037DF0E29A3B83D4D2FCE3E1BFC444F2A
