Buer Loader Found in an Unusual Email Attachment

By VIPRE Labs

Published: 2021-03-18 · Archived: 2026-04-05 19:45:07 UTC

The COVID-19 pandemic has resulted in people ramping up online activities working from home, online shopping and relying more on online services. Recently, we came across a spam email lurking in the wild. This spam email is disguised as a known logistics company and has an unusual attachment. Malicious attackers trick the victim into believing that the email is legitimate by using a legitimate domain in the sender's email address. The content is also properly constructed and also uses a known logo making it difficult to spot that it is a malicious email.


Figure 1.0 Spam email with .jnlp attachment

Figure 1.0 Spam email with .jnlp attachment

As threats become more prominent, we should always be cautious. These are some indicators that will show that this email is suspicious and not legitimate:


Figure 2.0 The email header

Figure 2.0 The email header

- Checking the email header, we can see that the "received from" which is in the green box in Figure 2.0, didn't match with the "from" field (the visible sender of the email). The "received from" data is the most reliable and it is where we can see the real sender of the email. Upon researching, the domain in the "received from" header is not related to DHL. With this, the email header is forged.
- An Additional checker is the Received-SPF: softfail. It says that the "domain of DHL.COM does not designate 45.88.105.192 as permitted sender". Upon checking, the IP address 45.88.105.192 in the "received from" is not also related to DHL.
- The attachment of the email is a .jnlp file is a Java Network Launch Protocol which is an unusual attachment for an email.

Analyzing the attachment

We will now proceed on the analysis of the jnlp file attachment that has a filename "invoice.jnlp". We said earlier that .jnlp stands for Java Network Launch Protocol, that's used for launching java applications from a hosted web server on a remote desktop client. Checking the jnlp file, we can see that the file will download invoice.jar from a web server hxxp://invoicesecure[.]net/documents when executed.


Figure 3.0 The jnlp file

Figure 3.0 The jnlp file

The downloaded file is an invoice.jar file which is a Java Archive file. When we tried to launch the file it will show this output:

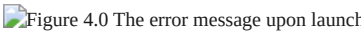
Figure 4.0 The error message upon launching invoice.jar

Figure 4.0 The error message upon launching invoice.jar

With this message, the victim will think that it was an error and will ignore the file. But upon analyzing the invoice.jar, we found out that this message is just a decoy. The attackers just made this technique to trick their victims and make the malware run without suspicion. Based on its code after showing an error message, it will start to read the data from "hxxp://invoicesecure[.]net/img/footer[.]jpg" and saved it as "C:\ProgramData\drvr32.exe". Then use Desktop.getDesktop().open() to open drvr32.exe.


Figure 5.0 The decompiled invoice.jar

Figure 5.0 The decompiled invoice.jar


Figure 6.0 The HTTP GET Request once invoice.jar was executed

Figure 6.0 The HTTP GET Request once invoice.jar was executed

The Buer Loader

The malicious downloaded file was named “drvr32.exe” and disguised as a legitimate xls viewer application:

Figure 7.0 Disguising as a legitimate file

This file was identified as a type of a malware loader known as Buer Loader. This loader was first seen in 2019 and commonly distributed through malicious spam email campaigns.

Figure 8.0 The buer loader

When executed, it will first create its installation folder “zsadsadsad” at the Startup folder and create a copy of itself in %AppData%. The created folder “zsadsadsad” contains LNK shortcut file. We decoded the LNK file to analyze all the available information it contains and we found out that it will link to the created copy.

Figure 9.0 The installation folder “zsadsadsad” and the lnk shortcut file

Figure 10.0 The decoded information of LNK file linking to the created copy

Throughout our analysis, we found out that this loader has an anti-analysis. It will check if the following DLLs are existing in the place where the malware is running:

Figure 11.0 The DLLs to check

As per checking, some of the checked DLLs above are related to anti-virus and debuggers.

Then, it will call functions like GetCurrentHwProfileA, GetComputerNameW, and GetVolumeInformation to collect the information of the infected machine. The collected information will be combined in an allocated memory and will be formatted using wsprintfw function.

Figure 12.0 Routine for formatting the collected information

Figure 13.0 The formatted string of victim’s machine information

After this, it will call other functions to retrieve more information of the infected machine and to use these information for the malware’s next actions:

- RtlGetVersion
- GetNativeSystemInfo
- GetComputerNameW
- GetDriveTypeA
- GetDiskFreeSpaceExA
- GetUserNameW
- NetWkstaGetInfo

All of the other retrieved information will be combined to the formatted string above and the output is this:

cb9f1daacc0545c0e5bf0c67ead614d24884570889cf7435572fa55e134b1012|bc31re1bs5a8d1fc4ddb3cc4b75594c31b8c00de3fdfa31fgg1ad15e87|x32|1|User|WIN-SPF5F5SH244|14/59|WORKGROUP|test|0

Then, this output will be formatted again using wsprintfw function and the result is this:

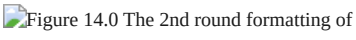

Figure 14.0 The 2nd round formatting of string of the victim’s machine information

After retrieving and formatting the needed information of the victim's machine, Buer Loader will make it to a base64 string:


Figure 15.0 Converting to base64 string

Figure 15.0 Converting to base64 string

Digging deeper into our analysis, we encountered InternetOpenA function to initialize a use of the WinINet functions. Then, it will try to open an http session to "verstudiosan[.]com" using InternetConnectW function.

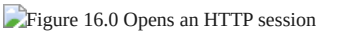
Figure 16.0 Opens an HTTP session

Figure 16.0 Opens an HTTP session

It has GET method to download additional malware and POST method to send the collected victim's machine information to the server:


Figure 17.0 HTTP POST Request method

Figure 17.0 HTTP POST Request method

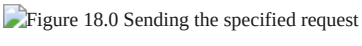
Figure 18.0 Sending the specified request

Figure 18.0 Sending the specified request

We searched the domain and found out that this domain was just recently created. We also learned that this domain is no longer reachable and possibly just used for malicious activity.


Figure 19.0 The recently created domain

Figure 19.0 The recently created domain

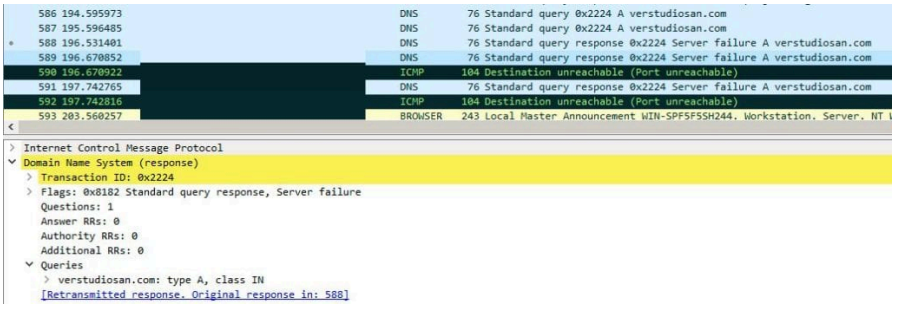

Figure 20.0 Unreachable server

Attack Flow


Attack Flow

VIPRE detects and prevents this kind of malware and associated infections.

IOCs:

- The Spam Email
  - 66f13fa2c9e34705bbbc4645462188ca57c0fdc3a17418c96c0ed9371055f3bc
- JNLP File
  - 368b409080e9389b342e33a014cd7daf3fd984fdc2b0e5ecc8ac4d180759a1c4
- Jar File
  - 064fe7ef429f373d38813a05c9d2286a86337c1fc1b12c740b729f1f76de1811
- PE File
  - dbdc38dee1c9c9861a36cf6462dca55dcef6c1f128b2270efd99d4347568292c
- Malicious website
  - verstudiosan[.]com
  - hxxp://invoicesecure[.]net/documents

Analysis by #Farrallel
