Posted on May 27, 2022

XLL Malware Distributed Through Email

Malware strains have been created and distributed in various forms and types. As such, the ASEC analysis team is actively monitoring and analyzing such changes to allow AhnLab products to detect them. This post will introduce XLL malware that was discovered being distributed last year.

XLL files are Microsoft Excel add-in files that operate with the extension .xll and can be opened by Excel. One thing to note is that the files are opened with MS Excel. This means users might mistake their forms as documents when they are actually DLL executables. The Excel files (.xlam and .xlsm) including the VBA macro that were previously introduced often are created with VBA, but the files discussed in this post are created with C programming language types. So while the form of the files is still DLL, the detailed configuration may change depending on the case that is compiled.

The XLL malware type was found to be distributed from July last year up till now. They are distributed through emails, and the malware that is ultimately executed varies, including info-stealer and ransomware.

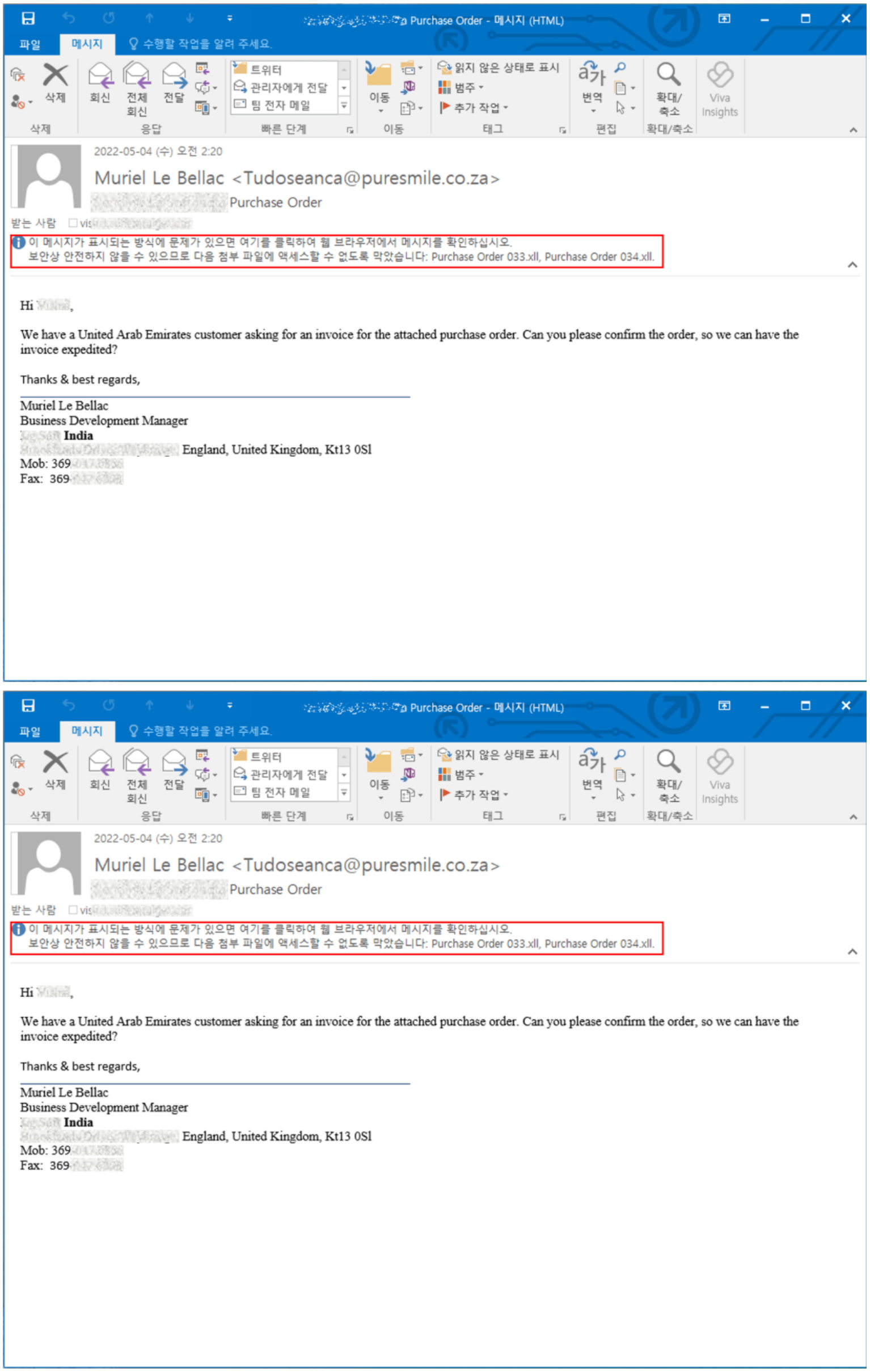


Figure 1. Email with .xll attachments blocked (Outlook 2016)

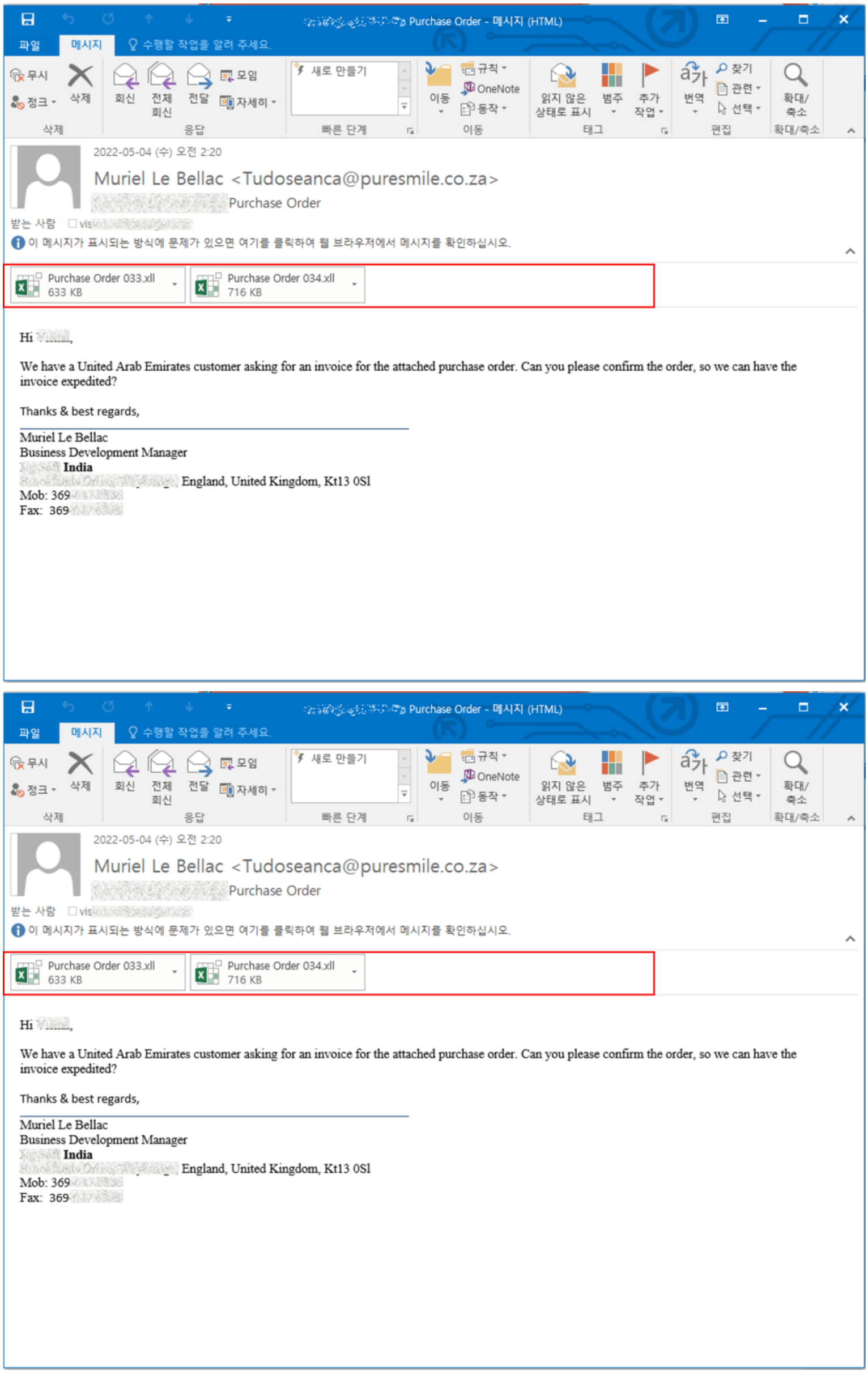


Figure 2. Email with .xll attachments unblocked (Outlook 2016)

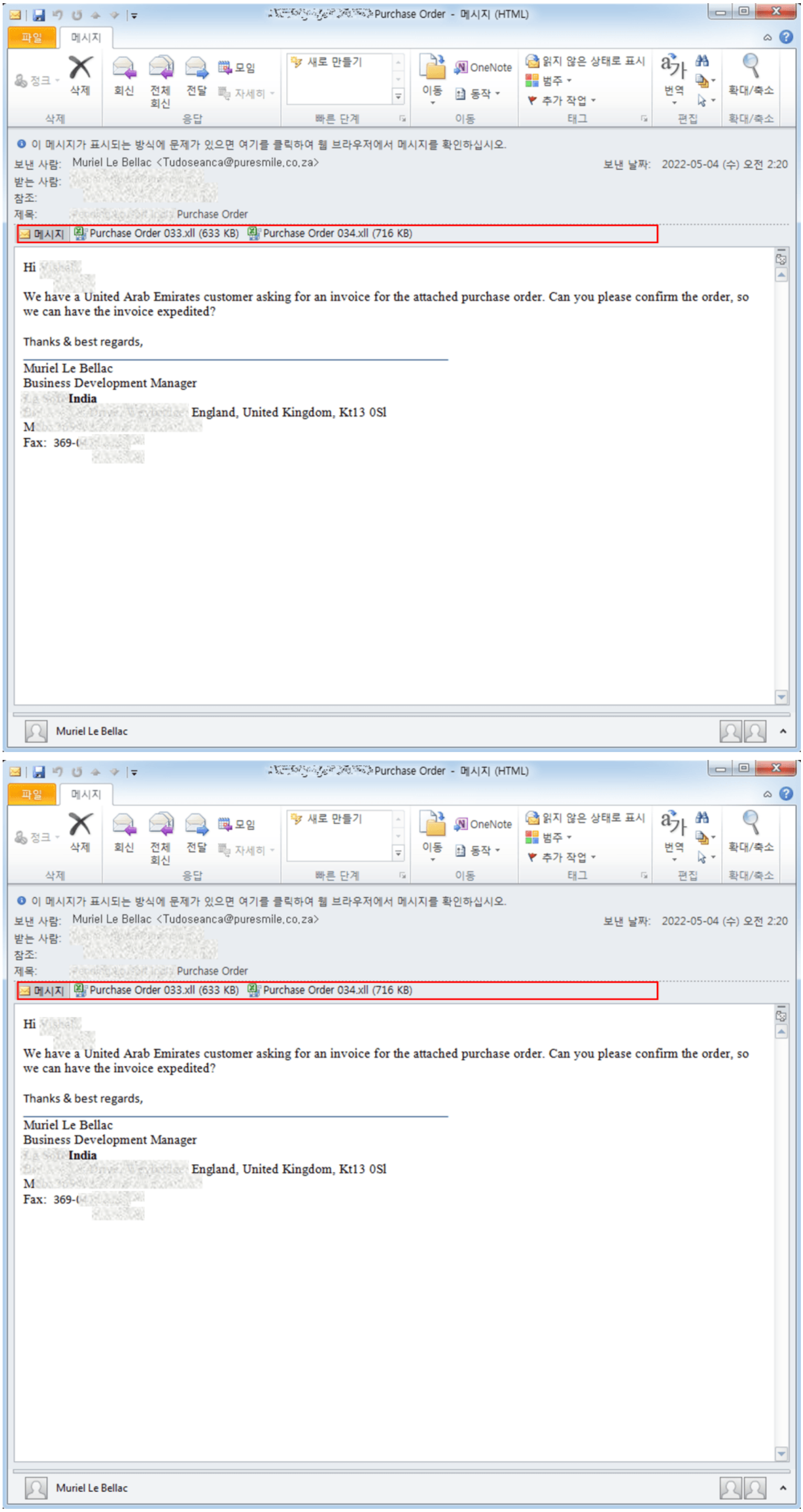


Figure 3. Email with .xll attachment (Outlook 2010)

As the latest version of Outlook blocks attachments of the file form mentioned in this post (see Figure 1), the block needs to be lifted to check the files (see Figure 2). Previous versions of Outlook allow you to check the attachments without prior adjustments (see Figure 3). Note that in a version that blocks the attachments, you have to manually change the registry as the block cannot be lifted in Outlook's default settings. Microsoft is also recommending users rename the extensions of blocked attachments to use them.

Outlook에서 차단되는 파일 형식

최신 버전 **Office 2007**

Microsoft Exchange Server 계정을 사용하는 경우 Exchange Server 관리자가 Outlook 보안 설정을 구성했다면 관리자에게 도움을 요청할 수 있습니다. Outlook에서 차단된 첨부 파일을 허용하도록 사서함의 보안 설정을 조정해 줄 것을 관리자에게 요청하세요.

Exchange Server 계정을 사용하지 않는 경우에는 고급 절차를 통해 일부 파일 형식의 차단을 해제할 수 있습니다. 이 절차에서는 Windows의 레지스트리를 편집합니다. 첨부 파일 형식의 차단 해제에 대한 자세한 내용은 Outlook에서 차단되는 첨부 파일에 대한 Microsoft 고객지원 문서를 참조하세요.

Outlook에서 차단되는 파일 형식

확장명	파일 형식
.ade	Access 프로젝트 익스텐션(Microsoft)
.adp	Access 프로젝트(Microsoft)
.app	실행 가능한 응용 프로그램
.application	ClickOnce 배포 매니페스트 파일
.appref-ms	ClickOnce 애플리케이션 참조 파일

. . .

.xll	Excel 추가 기능
.xnk	Exchange 공용 폴더 바로 가기

Outlook에서 차단되는 파일 형식

최신 버전 Office 2007

Microsoft Exchange Server 계정을 사용하는 경우 Exchange Server 관리자가 Outlook 보안 설정을 구성했다면 관리자에게 도움을 요청할 수 있습니다. Outlook에서 차단된 첨부 파일을 허용하도록 사서함의 보안 설정을 조정해 줄 것을 관리자에게 요청하세요.

Exchange Server 계정을 사용하지 않는 경우에는 고급 절차를 통해 일부 파일 형식의 차단을 해제할 수 있습니다. 이 절차에서는 Windows의 레지스트리를 편집합니다. 첨부 파일 형식의 차단 해제에 대한 자세한 내용은 Outlook에서 차단되는 첨부 파일에 대한 Microsoft 고객지원 문서를 참조하세요.

Outlook에서 차단되는 파일 형식

확장명	파일 형식
.ade	Access 프로젝트 익스텐션(Microsoft)
.adp	Access 프로젝트(Microsoft)
.app	실행 가능한 응용 프로그램
.application	ClickOnce 배포 매니페스트 파일
.appref-ms	ClickOnce 애플리케이션 참조 파일
. . .	
.xll	Excel 추가 기능
.xnk	Exchange 공용 폴더 바로 가기

Figure 4. File types blocked in Outlook

● Purchase Order 033.xll and Purchase Order 034.xll

The attachments ‘Purchase Order 033.xll’ and ‘Purchase Order 034.xll’ from Figures 1, 2, and 3 have the following features. First, as explained earlier, you can see the files’ form is DLL as shown in Figure 5. When the files are run (as .xll), they are opened with Microsoft Excel (see Figure 6). Clicking ‘Enable this add-in for this session only.’ will activate the behavior, while clicking ‘Leave this add-in disabled.’ will not activate the behavior. As such, you can click the right button to avoid the malware infection if you accidentally ran an unconfirmed XLL file.

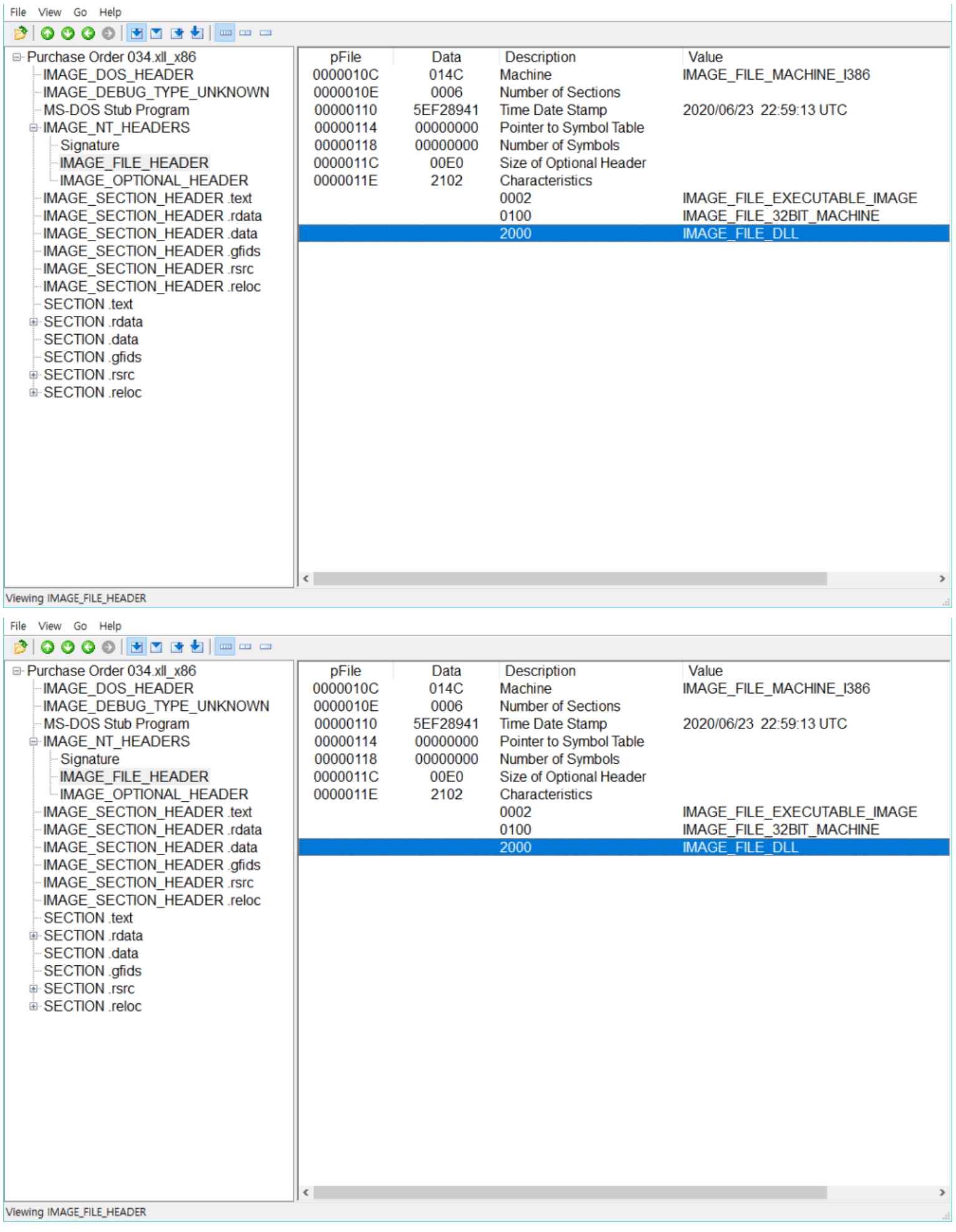


Figure 5. Form of Purchase Order 034.xll

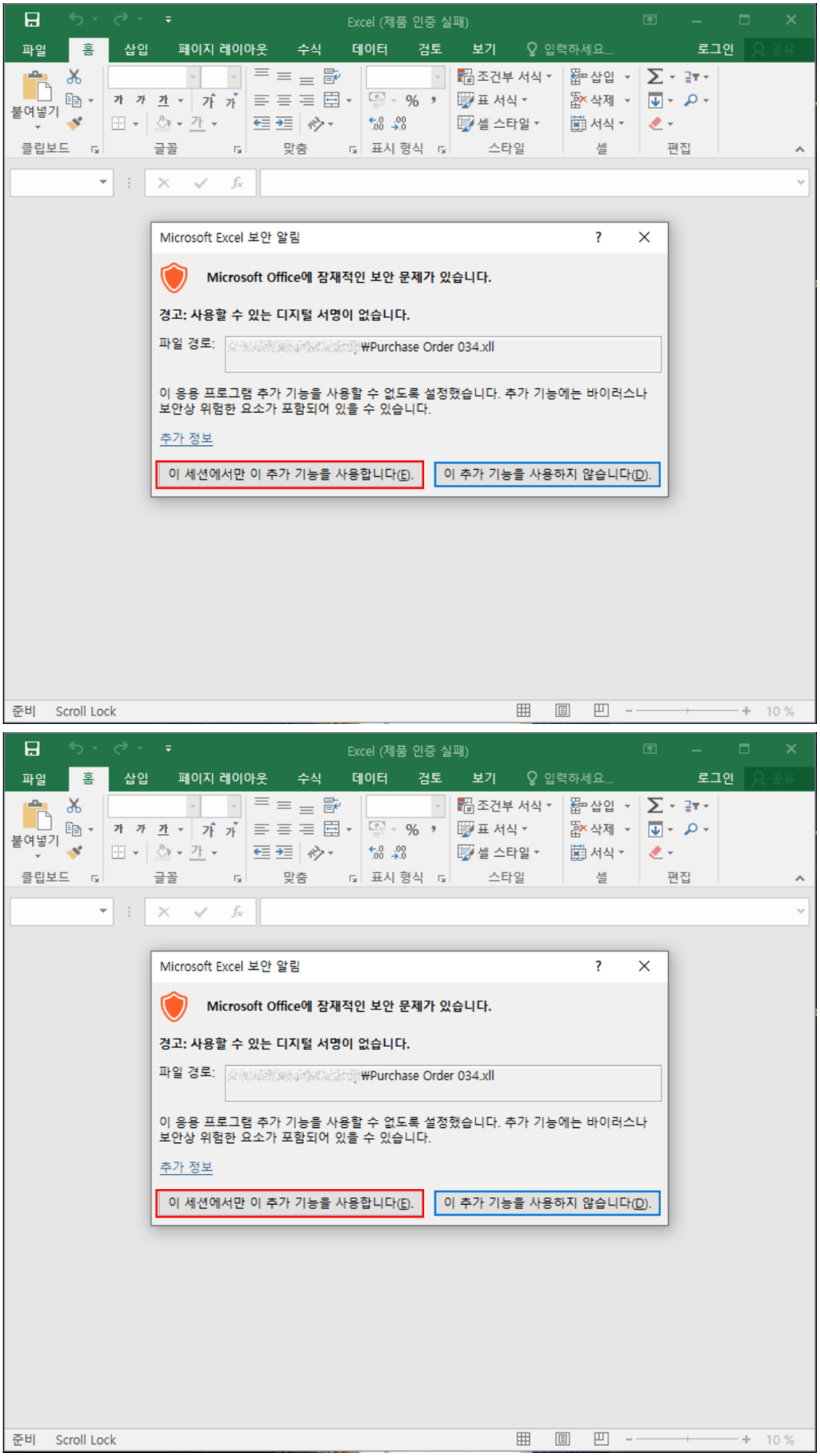


Figure 6. Purchase Order 034.xll executed

If you do not know the extension of the file, it might be difficult to know if the file is an XLL file by looking at its form since the executable has a DLL structure. However, XLL files have an Export function named ‘xlAutoOpen’. It is a callback function that needs to be configured in every XLL function. The function is required to run XLL.

As for ‘Purchase Order 033.xll’ and ‘Purchase Order 034.xll’, you can check the DLL that performs essential features if you extract the internal data with an XLL file compiled with an open-source program named ‘Excel-DNA.’ The DLL is created with .net.

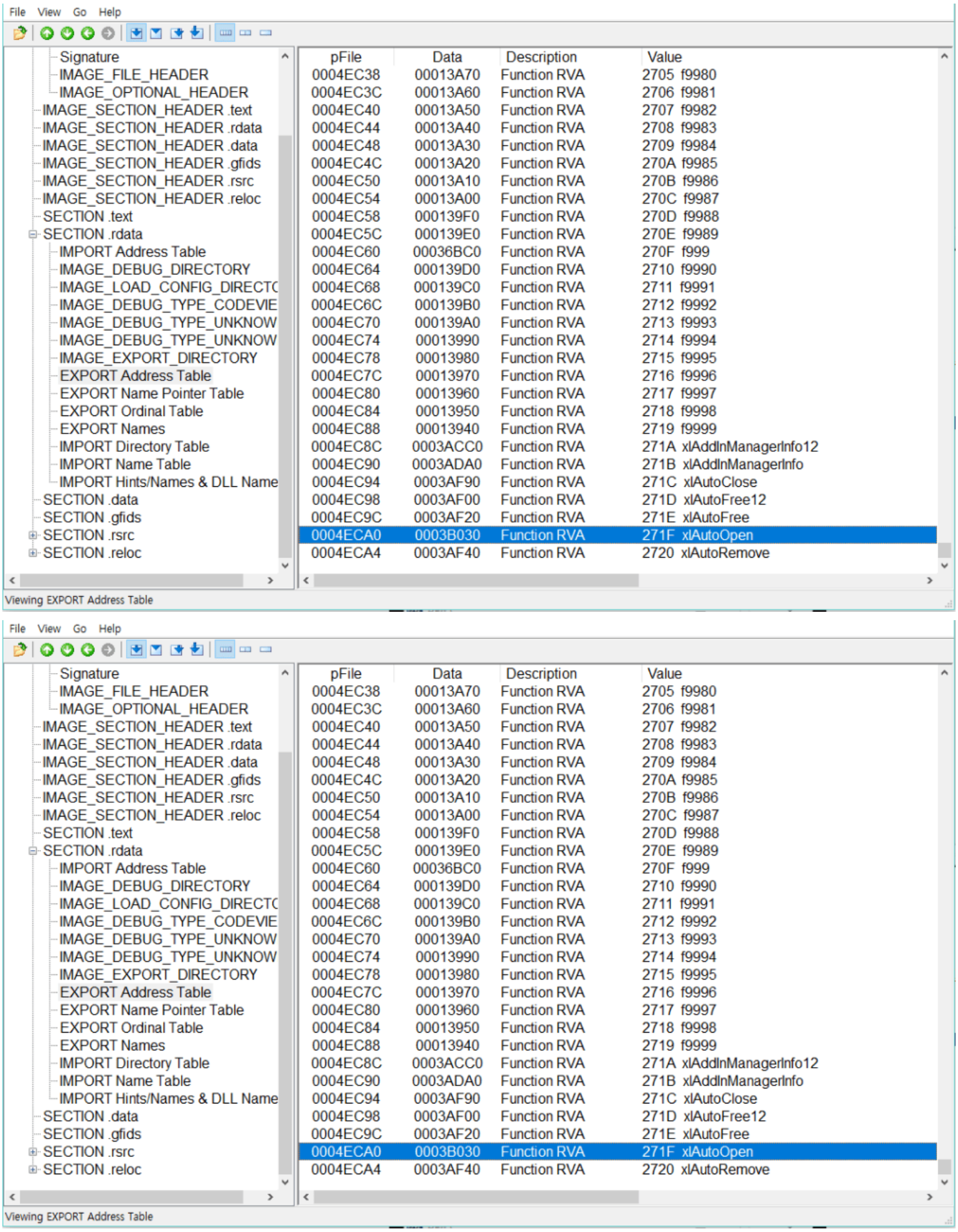


Figure 7. xlAutoOpen Export function of XLL file

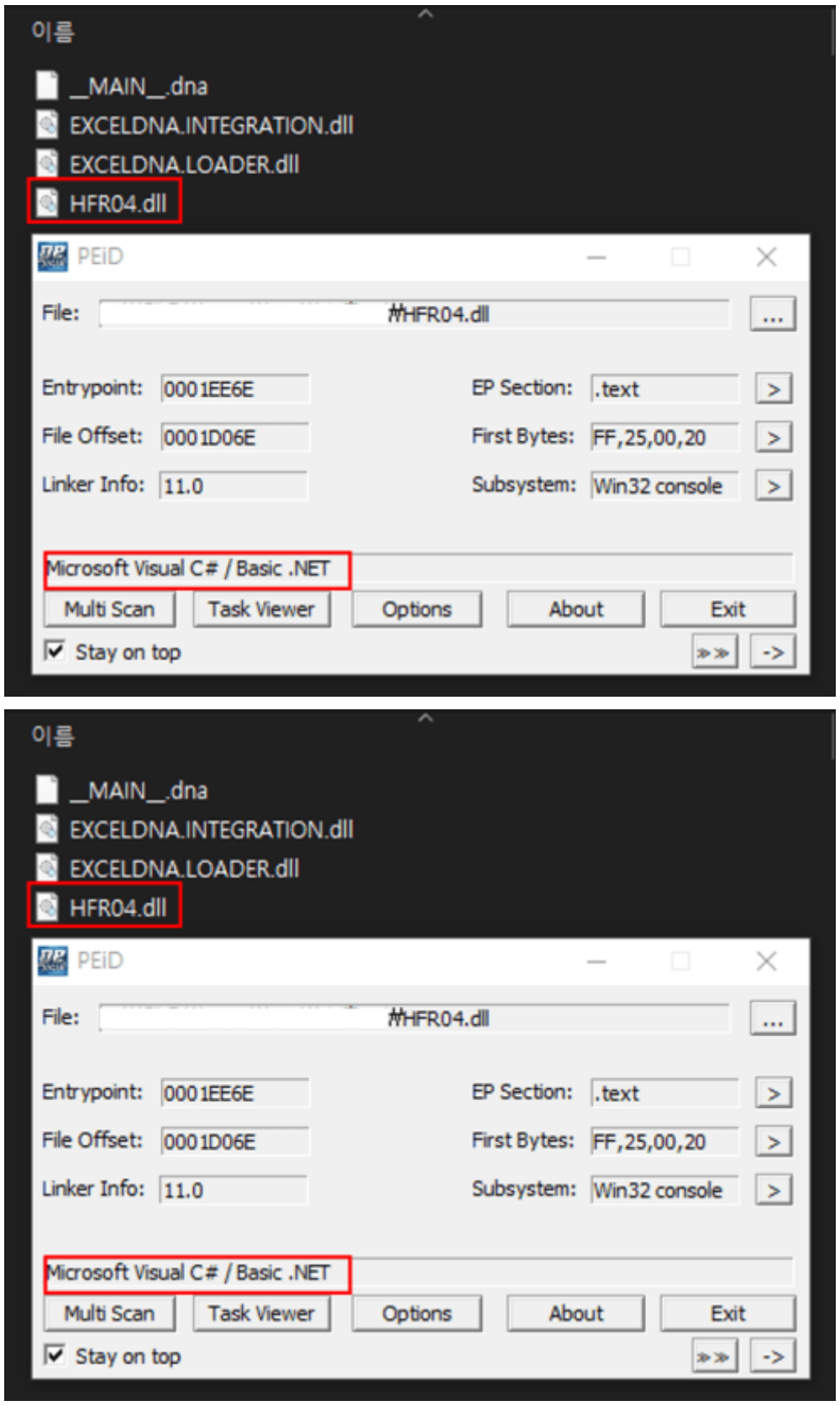


Figure 8. HFR04.dll (.net) internally extracted from Purchase Order 034.xll

Figure 9. Purchase Order 034.xll attempting to access the network

HFR04.dll inside Purchase Order 034.xll attempts to access the network (see Figure 9), downloading additional malware strains from the URL shown below. As it does not download any meaningful data from the URL, the team could not check the additional features. Yet looking at the XLL malware

strains that were distributed since July last year shows that it will likely download ransomware and info-stealer types. The following samples show instances of such malware types being downloaded.

– hxxps://www.mcroller[.]com/express.exe

● Resume.xll

The file distributed with the name ‘Resume.xll’ was also compiled with Excel-DNA. Like the files introduced earlier, the internally extracted DLL is also a .net file. This file accesses the network to download additional malware. AhnLab’s internal record shows that ransomware was downloaded from the following URL.

– hxxp://104.161.34[.]171/library.exe

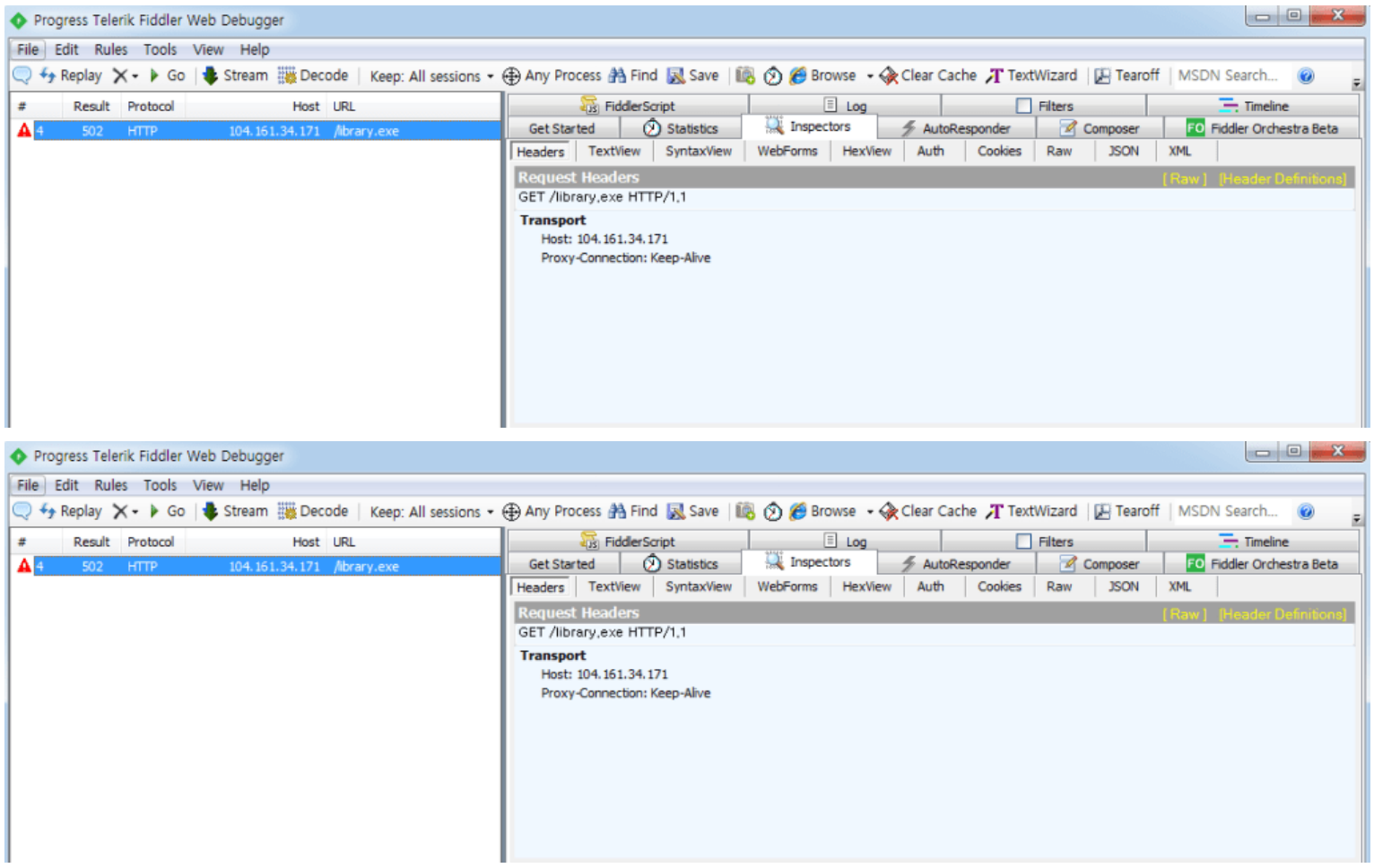
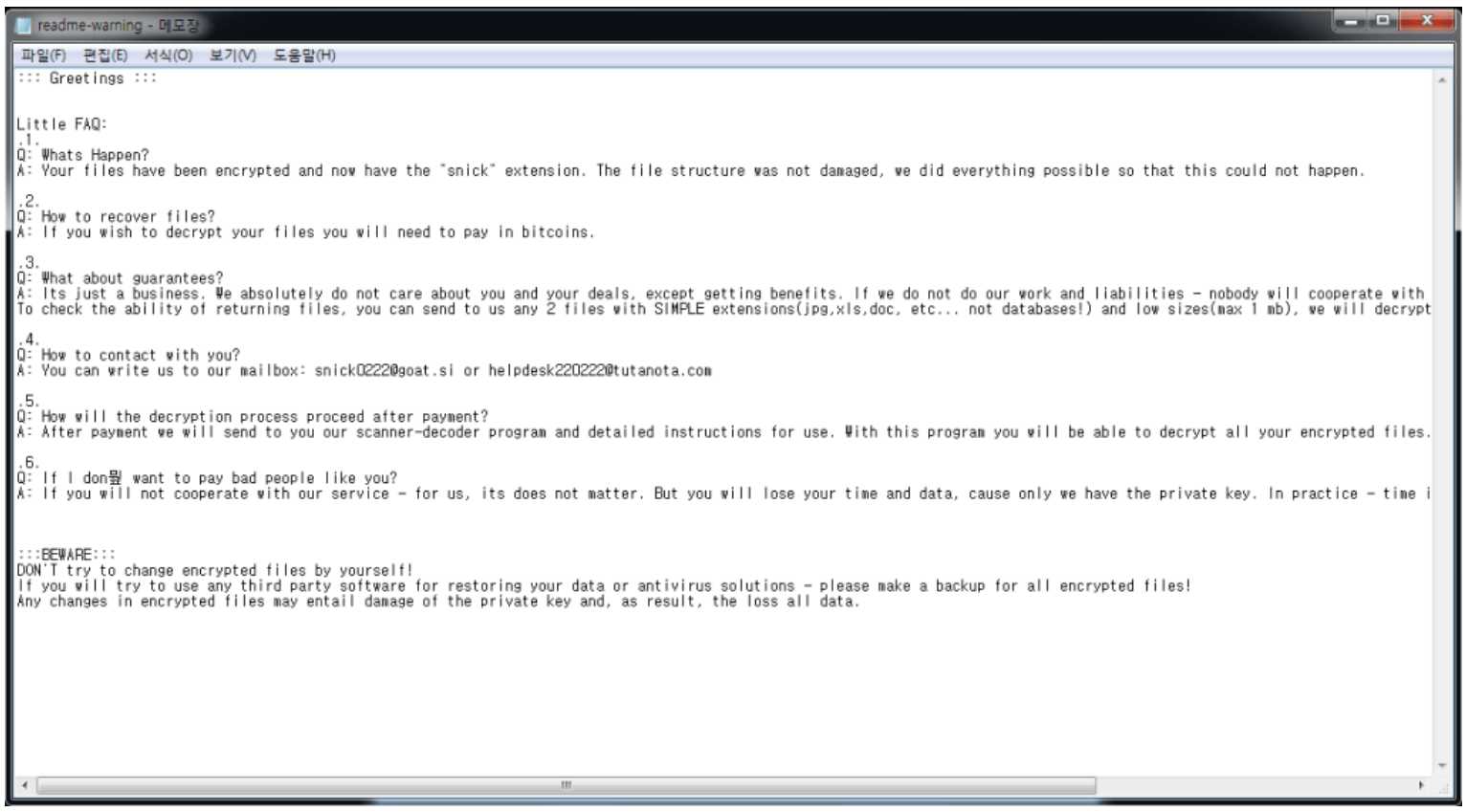


Figure 10. Resume.xll attempting to access the network



readme-warning - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
::: Greetings :::
Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted and now have the "snick" extension. The file structure was not damaged, we did everything possible so that this could not happen.
.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in bitcoins.
.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt
.4.
Q: How to contact with you?
A: You can write us to our mailbox: snick0222@goat.si or helpdesk220222@tutanota.com
.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.
.6.
Q: If I don뭘 want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause only we have the private key. In practice - time i
:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.

Figure 11. Carlos ransomware infection

● MV SEAMELODY.xll

The XLL file distributed with the name ‘MV SEAMELODY.xll’ acts as a downloader as well. This file also has its internal core DLL perform majors features. The following figure shows its code.

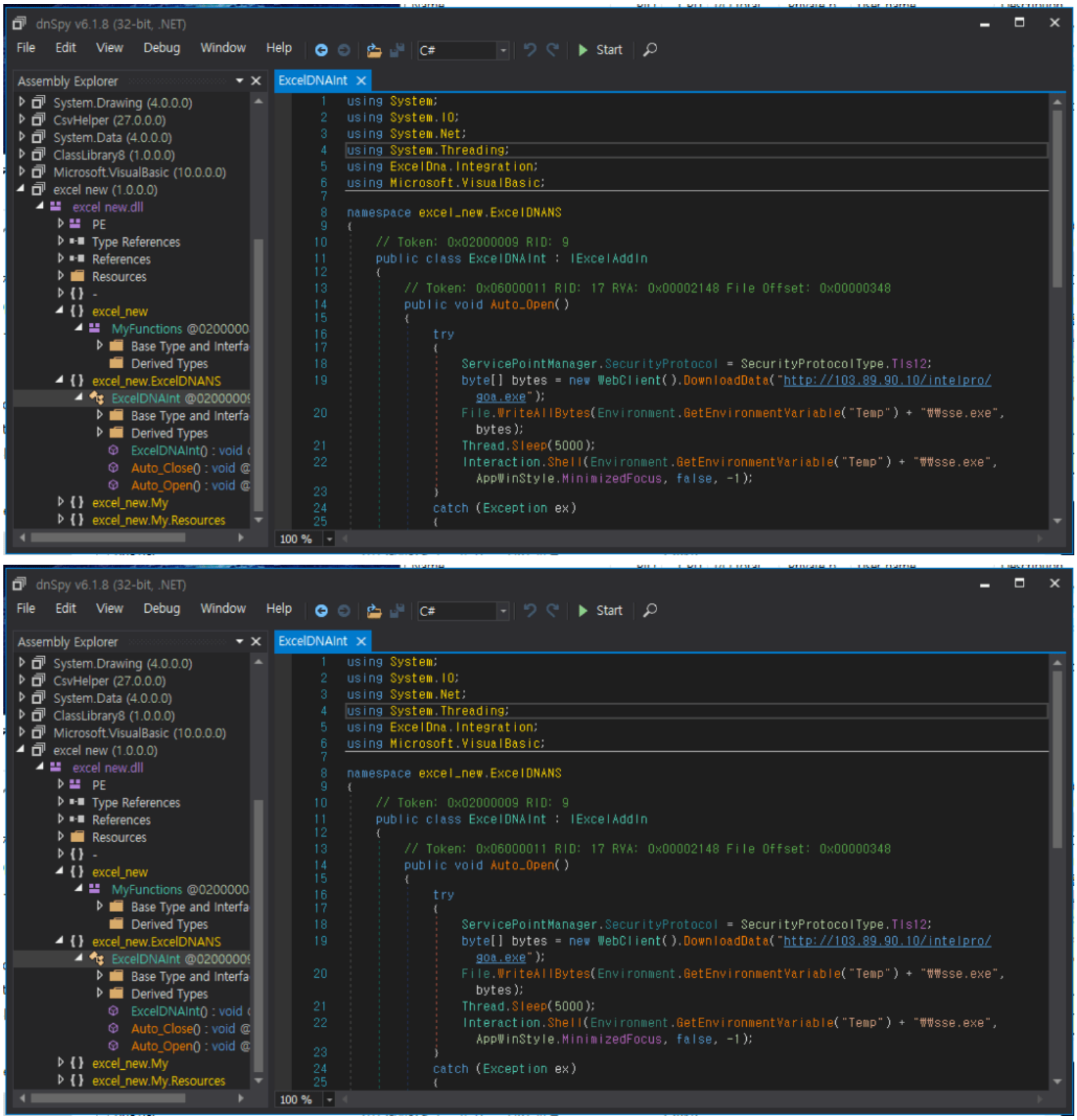


Figure 12. Code for DLL inside MV SEAMELODY.xll

— hxxp://103.89.30[.]10/intelpro/goa.exe

The file attempts to access the URL to download additional malware. The record shows that the file downloaded from the URL is Lokibot.

As you can see, now there is one more distribution method of Info-stealer and ransomware, the two malware types that take a significant portion of the recent malware distribution. Users should be cautious when they view attachments of suspicious emails. Furthermore, they must keep their anti-malware software updated to the latest version.

AhnLab V3 detects and blocks the malware strains using the aliases below.

[File Detection]

- Downloader/Win.MalXll.R490565
- Downloader/Win.MalXll.R466354
- Trojan/Win.Agent.C5025449
- Ransomware/Win.Carlos.C5025252

[IOC Info]

- c181e7eaacbcfe010375a857460a76c6
- 128ab502ed4f070abea44fd42b24f9d3
- 1f24e9fa558c3394935c9b41ffad2034
- 4685703aa9868c5f71da11422ccf30e8
- d599aecaa32e0b0b41f4a688f85388c6
- hxxps://www.mcroller[.]com/express.exe

- hxxp://104.161.34[.]171/library.exe
- hxxp://103.89.30[.]10/intelpro/goa.exe

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:InfoStealer, phishing, Phishing email, Ransomware, XLL malware