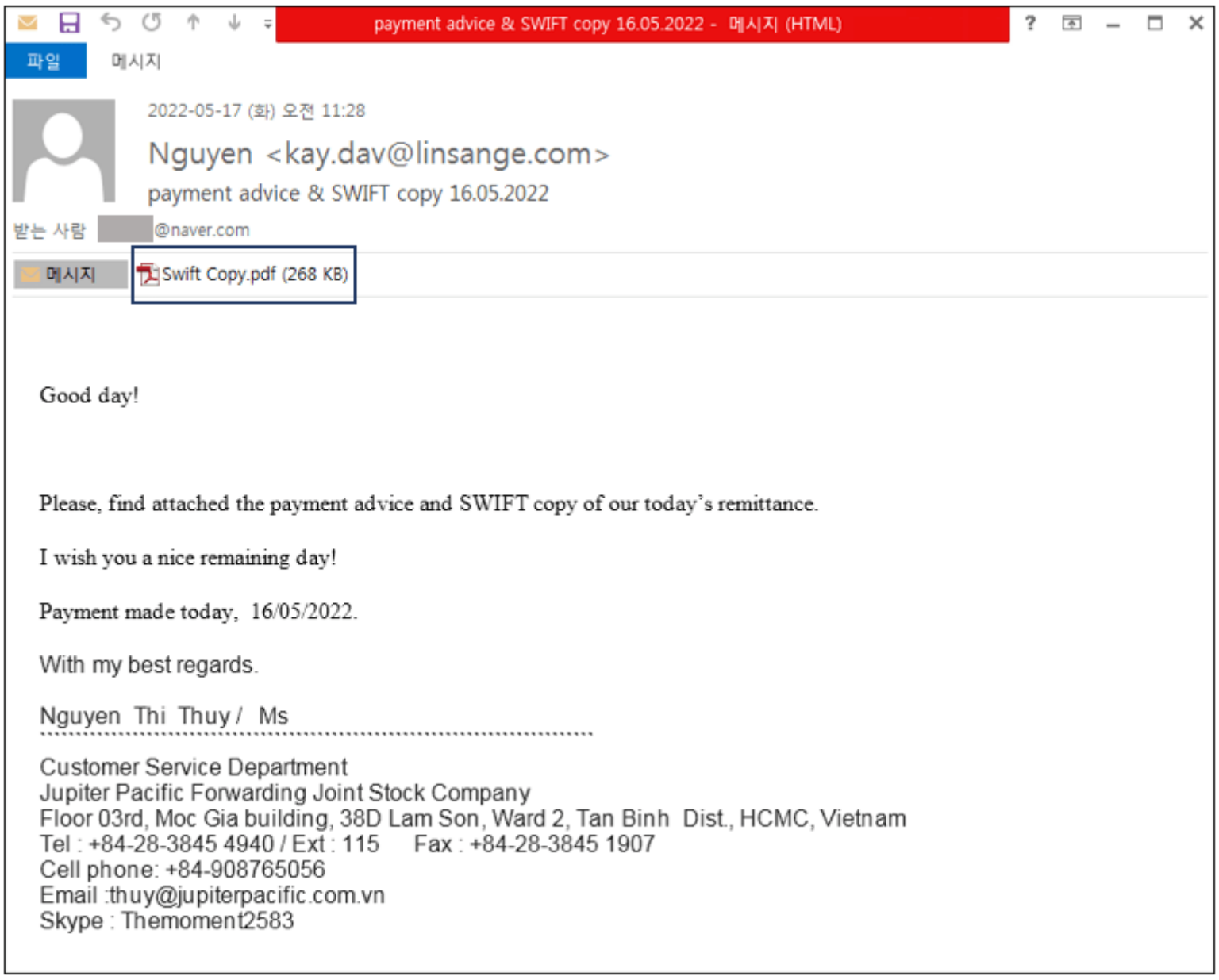
Posted on May 25, 2022

Method that Tricks Users to Perceive Attachment of PDF File as Safe File

The ASEC analysis team has discovered the distribution of info-stealer malware using Attachment feature of PDF files. This attack method was discovered previously, but as the malware of this type has resurfaced and is being actively distributed, the team would like to share the information. Note that the attacker used a simple trick of using the attachment's name to deceive users.



payment advice & SWIFT copy 16.05.2022 - 메시지 (HTML)
파일
메시지
2022-05-17 (화) 오전 11:28
Nguyen <kay.dav@linsange.com>
payment advice & SWIFT copy 16.05.2022
받는 사람 @naver.com
메시지
Swift Copy.pdf (268 KB)
Good day!
Please, find attached the payment advice and SWIFT copy of our today's remittance.
I wish you a nice remaining day!
Payment made today, 16/05/2022.
With my best regards.
Nguyen Thi Thuy / Ms
Customer Service Department
Jupiter Pacific Forwarding Joint Stock Company
Floor 03rd, Moc Gia building, 38D Lam Son, Ward 2, Tan Binh Dist., HCMC, Vietnam
Tel : +84-28-3845 4940 / Ext : 115 Fax : +84-28-3845 1907
Cell phone: +84-908765056
Email :thuy@jupiterpacific.com.vn
Skype : Themoment2583

Figure 1. Phishing e-mail with PDF attachment

Acrobat Reader has a feature of adding attachments to PDF files. Files with extensions such as .bin/.exe/.bat/.chm are blacklisted and cannot be attached because they are considered threats. For other files that do not exist in the default blacklist and whitelist, a message box that requires the user's decision appears. The attacker exploited this aspect of the software.

Upon running the PDF file attached to the e-mail, an intentionally blurred image is displayed, and a security warning message of 'Open file' appears due to Adobe Reader's default setting. This is a warning message for running the attachment of the PDF, and the filename appears directly on the message box. The sentence looks unnatural in Korean PC environment (see Figure 2), but if the user runs the PDF file in English PC environment (see Figure 3), the user can easily find out the intention of the attacker.

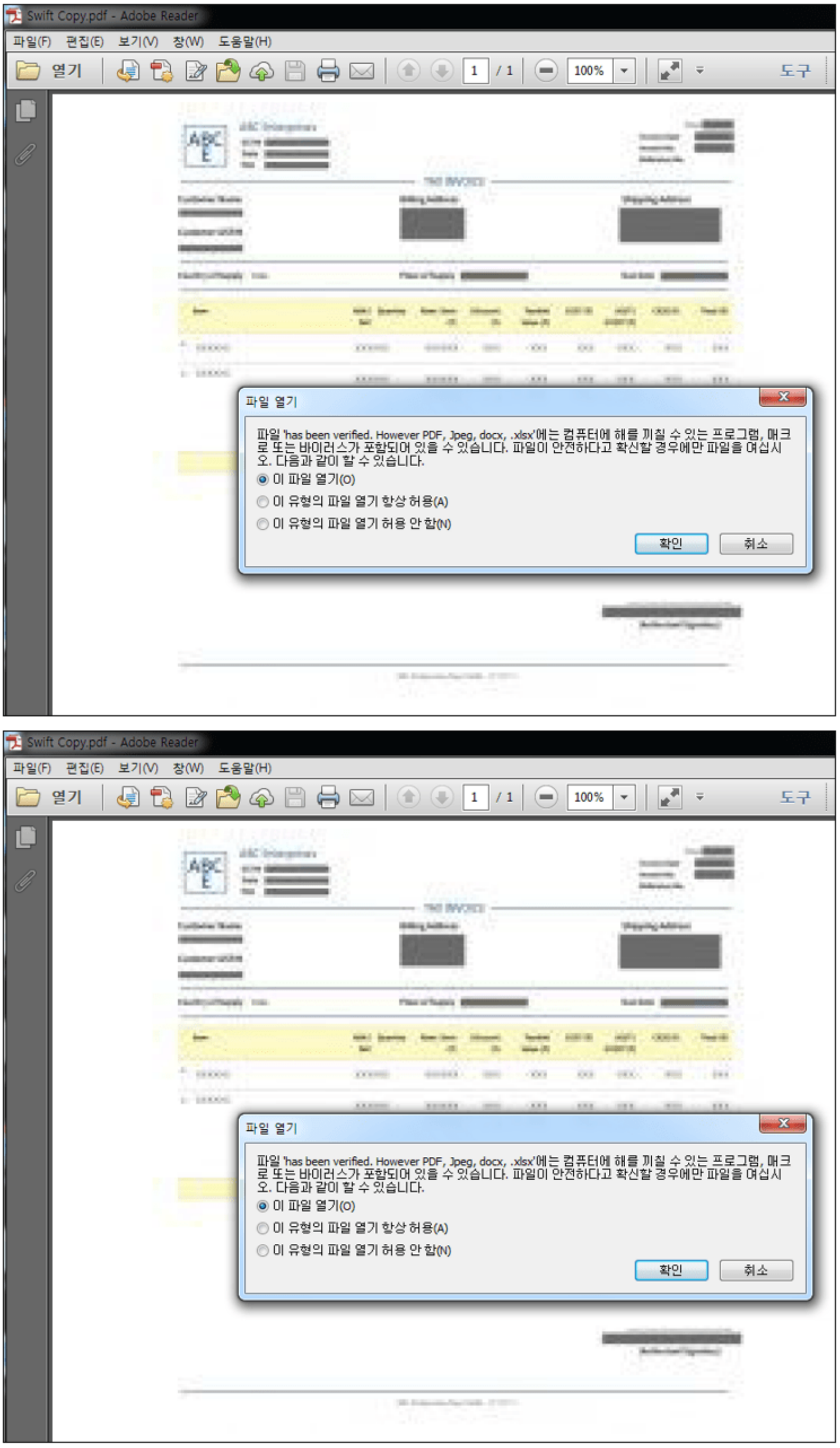


Figure 2. When running PDF file in Korean PC environment

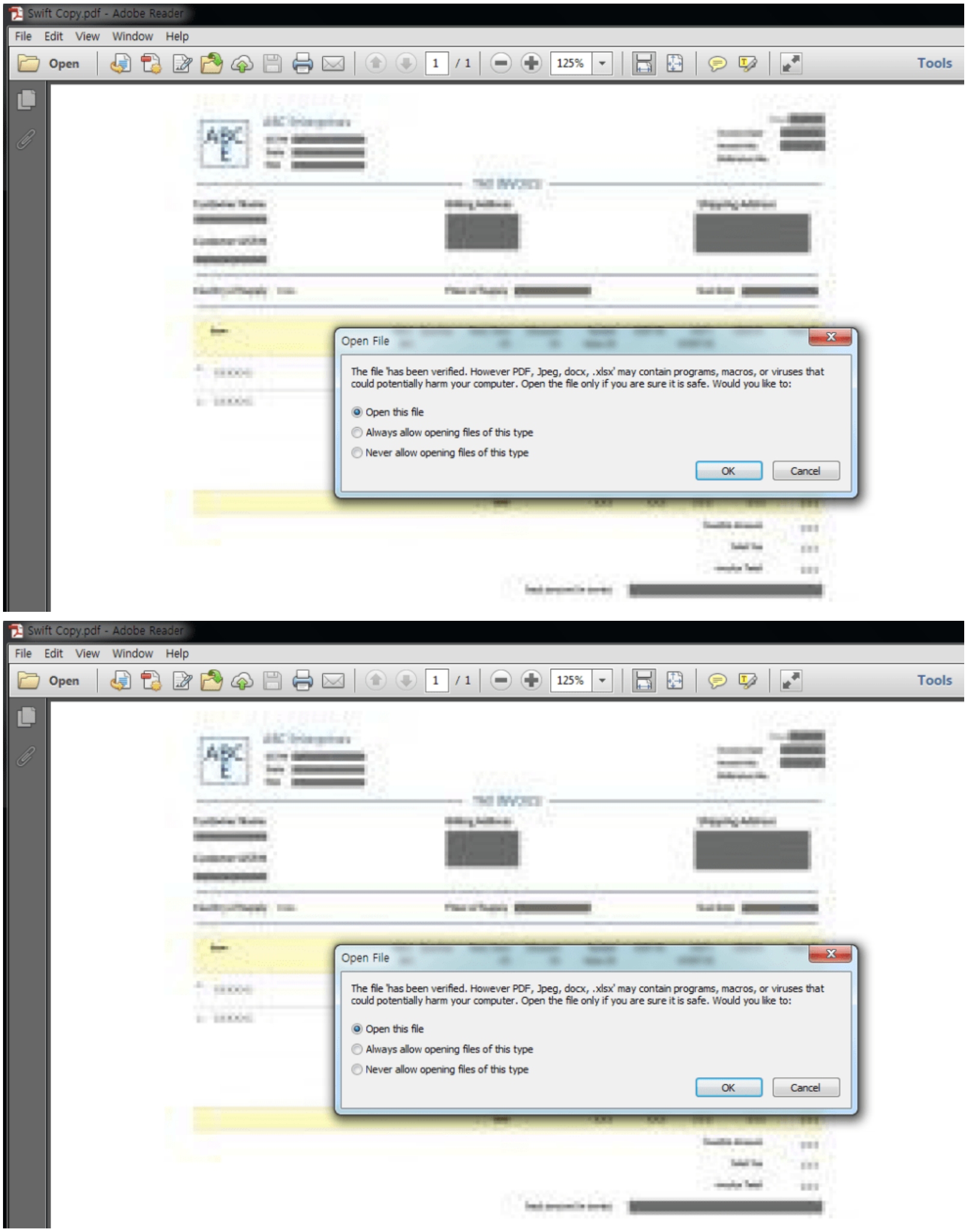


Figure 3. When running PDF file in English PC environment

The file attached to PDF is an Excel file with the filename: ‘has been verified. However PDF, jpeg, docx, .xlsx,’ and ignoring apostrophe that comes after “The file” in the message box forms a natural message like below. If the user does not read the file carefully, it is likely that they will think of it as a typical security message.

If the filename is ‘has been verified.’ ‘However PDF,’ ‘jpeg,’ ‘docx,’ ‘.xlsx’,

The file ‘has been verified. However PDF, jpeg, docx, .xlsx’ may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to: — Open this file — Always allow opening files of this type — Never allow opening files of this type → (User-executed) file is a (normal) file, but file with PDF, jpeg, docx, xlsx extension may contain malicious program, macro, virus, etc.

It appears that the attacker wrote this message after considering the possibility that the user may realize that the file is malware if the filename is the one that is commonly used in malware distribution (e.g. Quotation.xlsx) despite the same attachment being used, and promptly block the access to Acrobat Reader’s open file settings.

If the filename is Quotation.xlsx

The file ‘Quotation.xlsx’ may contain programs, macros, or viruses that could potentially harm your computer. Open the file only if you are sure it is safe. Would you like to: — Open this file — Always allow opening files of this type — Never allow opening files of this type → ‘Quotation.xlsx’ file may contain malicious programs, malicious macro, or virus that may harm the PC.

Filename of attachment inside the PDF file of this type are created to trick users. XLSX files as well as DOCX files have been confirmed as attachment, and each file utilized malicious elements that are commonly employed in Excel and Word type malware.

- has been verified. However PDF, jpeg, docx, .xlsx
- has been verified. However PDF, jpeg, xlsx, .docx
- is scanned and Verified. However PDF, docx, .xlsx
- is verified. However PDF, jpeg, Docx, .xlsx

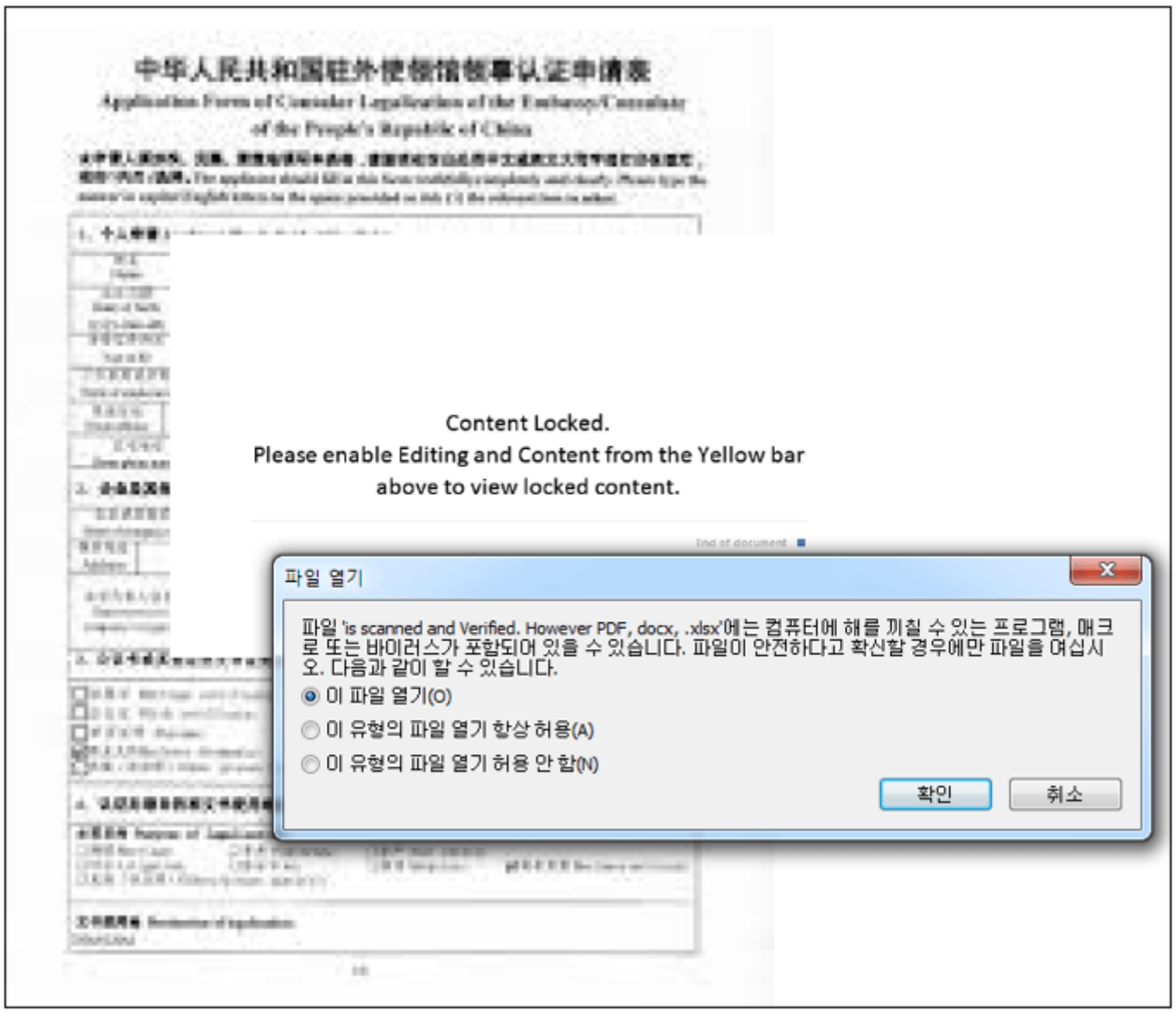


Figure 4. Attachment inside PDF file with same type but slightly different filename

When the Excel file is run, it connects to the external network via the formula editor (EQNEDT32.EXE) vulnerability and downloads the malware. The malware strains that have been confirmed over half a month of May were infostealer such as FormBook and Lokibot. FormBook and Lokibot are malware strains that consistently ranked high in ASEC weekly statistics. It is confirmed that they are being distributed through more meticulous means.

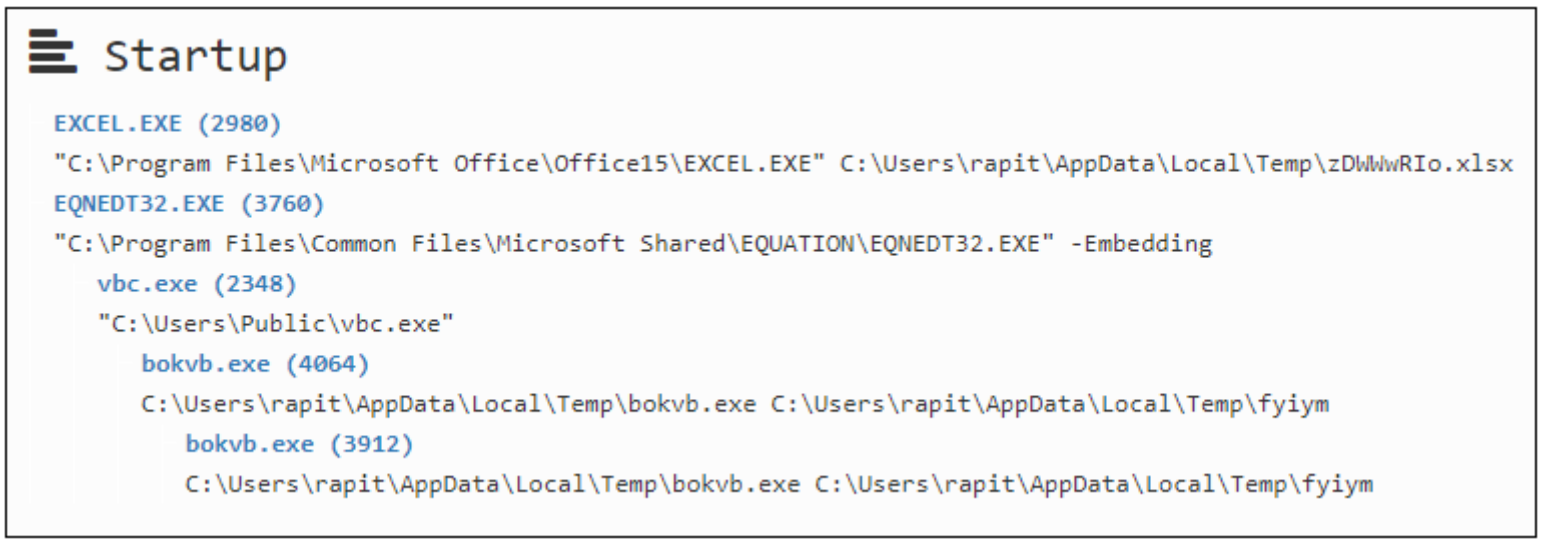


Figure 5. RAPIT process tree of Excel file

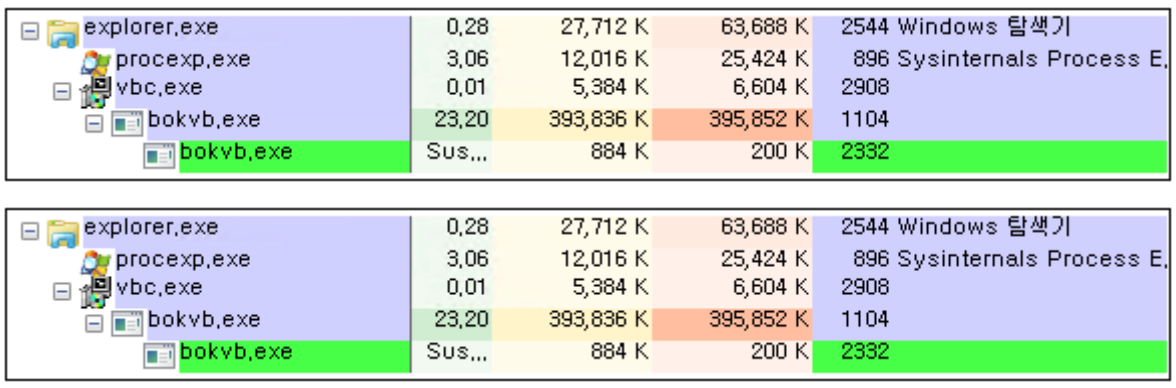


Figure 6. Lokibot (bokvb.exe) that is run by malware (vbc.exe) in NSIS form

To check the execution flow of the ‘has been verified. However PDF, jpeg, docx, .xlsx‘ file attached to the PDF file, the team saved the Excel attachment separately and executed it to check the process tree shown above. First, the malware (vbc.exe) in the form of NSIS (Nullsoft Scriptable Install System) is downloaded from an external URL via the formula editor (EQNEDT32.EXE) vulnerability, followed by the final malware (bokvb.exe) that is dropped and run. This file is run at the end and has been confirmed as Lokibot.

There have been cases of the attacker using Word files as well as Excel files that exploit the formula editor vulnerability. (Filename: has been verified. However PDF, jpeg, xlsx, .docx)

Figure 7. External URL that exists within document.xml.rels

The shortened URL that exists in document.xml.rels redirects to the final URL where the additional malware can be downloaded. An RTF file is downloaded from the final URL. The RTF file also adopts the same execution flow of using the formula editor vulnerability to download the NSIS malware.

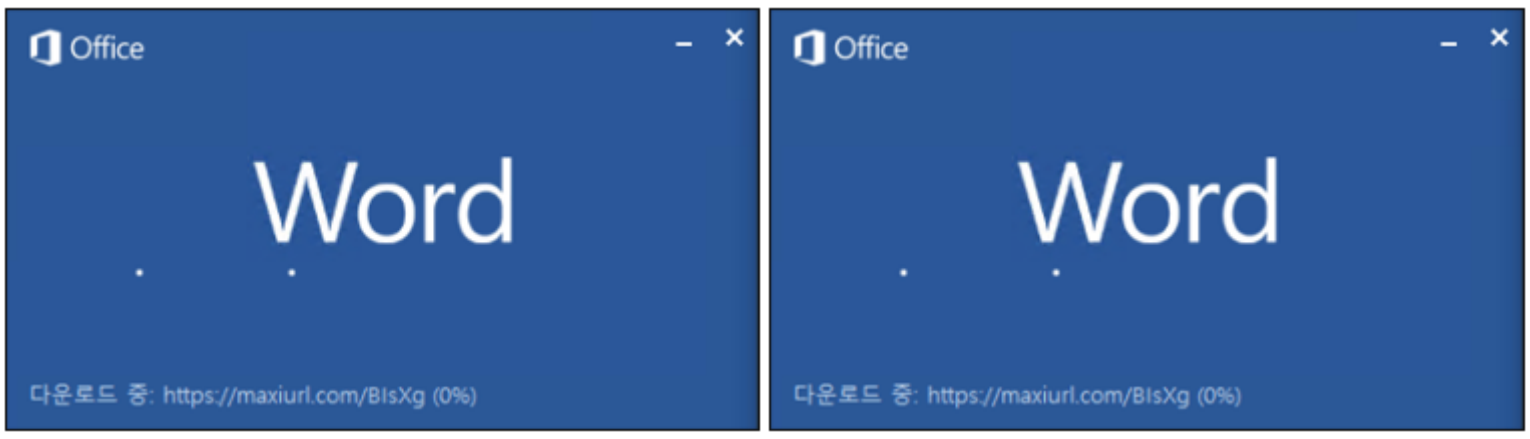


Figure 8. Word file attempting to connect to External URL (has been verified. However PDF, jpeg, xlsx, .docx)

Figure 9. Information of internal Word file saved in Acrobat Temp folder

- Shortened URL: hxxps://shorted[.]pro/stumwd
- Final URL: hxxp://172.245.163[.]188/document_shipping/document_g010.doc (RTF download)

The PC environment in which the PDF file is run may not be in English, but there is also a high chance that the user may click the confirm button (Open this file (O)) without paying attention to the message box that is created when opening the PDF file. Users can prevent the attachment file from being run instantly by selecting the third radio button of the message box and selecting the option 'Do Not Allow of Opening of This File Type (N).' Afterward, the user can check the information of the attachment again by clicking the clip-shaped tab on the tab to the left. (The default settings can be restored via Edit — Default Settings 'Trust Manager' menu.)

Recently however, there have been attackers distributing EML to Korean users. Extreme caution is advised for users when ultimately running the attachment inside received mails.

AhnLab's anti-malware software detect and block the malware above using the aliases below.

[File Detection] OLE/Cve-2017-0199.Gen OLE/Cve-2018-0798.Gen RTF/Malform-A.Gen Exploit/Pdf.Generic XML/Dloader Trojan/Win.NSISInject.R491618 Trojan/Win.NSISInject.R487995 Trojan/Win.FormBook.R492664 Trojan/Win.Generic.R481309

[IOC] 2d418caa178a376491815af16535ee08 (PDF) 374b79c1e46034ad1e3625c99195c113 (has been verified. However PDF, Jpeg, docx, .xlsx) hxxp://23.94.159[.]221/800/vbc.exe 4f2b5d6712ca51ba7619581acc9e6c06 (vbc.exe, NSIS) 016471d2742c31adedd647c6ee2022c1 (bokvb.exe / Lokibot) hxxp://hyatqfuh9olahvxf[.]ga/Legend/fre.php (Lokibot C2) 947ad46aa4cfc0eaf59fd7781aadc039 (PDF) c790888adcb84f9add8288d3634103da (has been verified. However PDF, Jpeg, xlsx, .docx) hxxp://172.245.163[.]188/document_shipping/document_g010.doc 53edca969843ae183610def08b00f022

(RTF) hxxp://172.245.163[.]188/crypted%20exes/ge010.exe 1bc2e6b3bcfc05766b833d0ee1bd9638 (ge010.exe, NSIS) a8cd72078de5d385315aa7b699e69ef9 (yphxlgsy.exe / Lokibot) hxxp://sempersim[.]su/ge10/fre.php (Lokibot C2)

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

Categories:Malware Information

Tagged as:Formbook, InfoStealer, LOKIBOT, malware, pdf malware, phishing