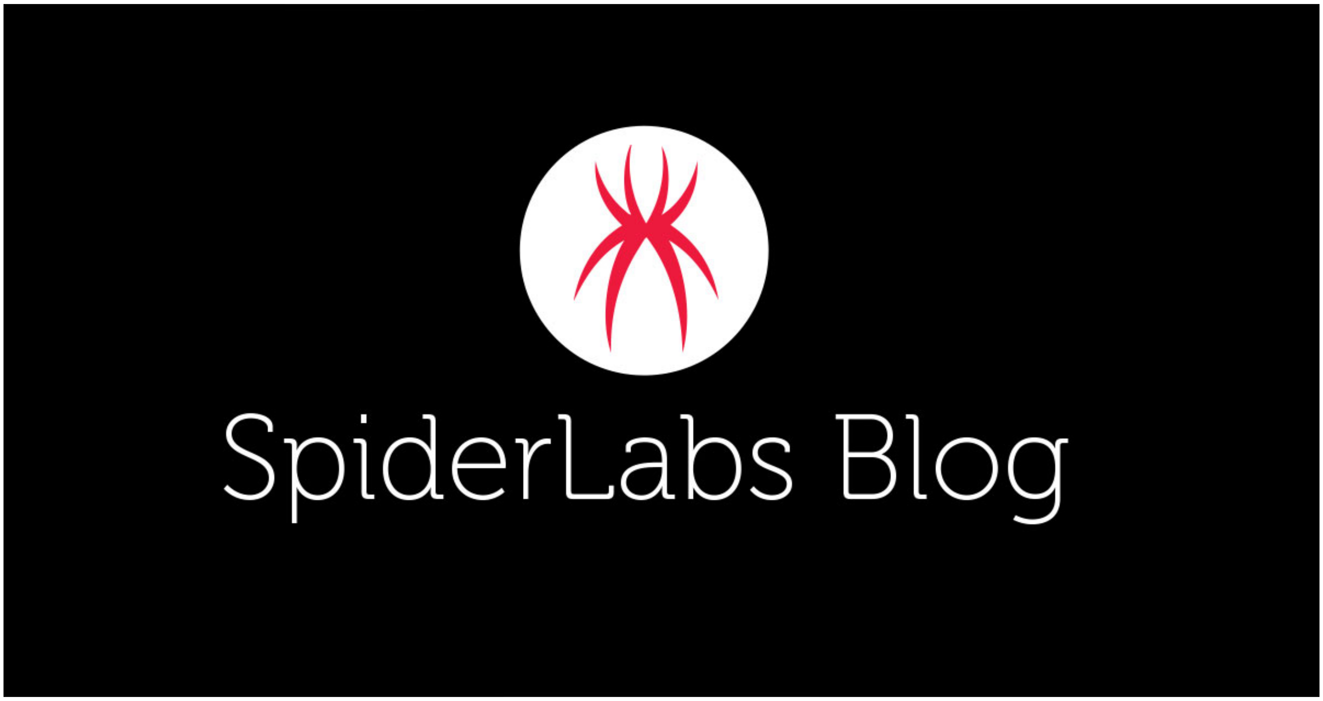
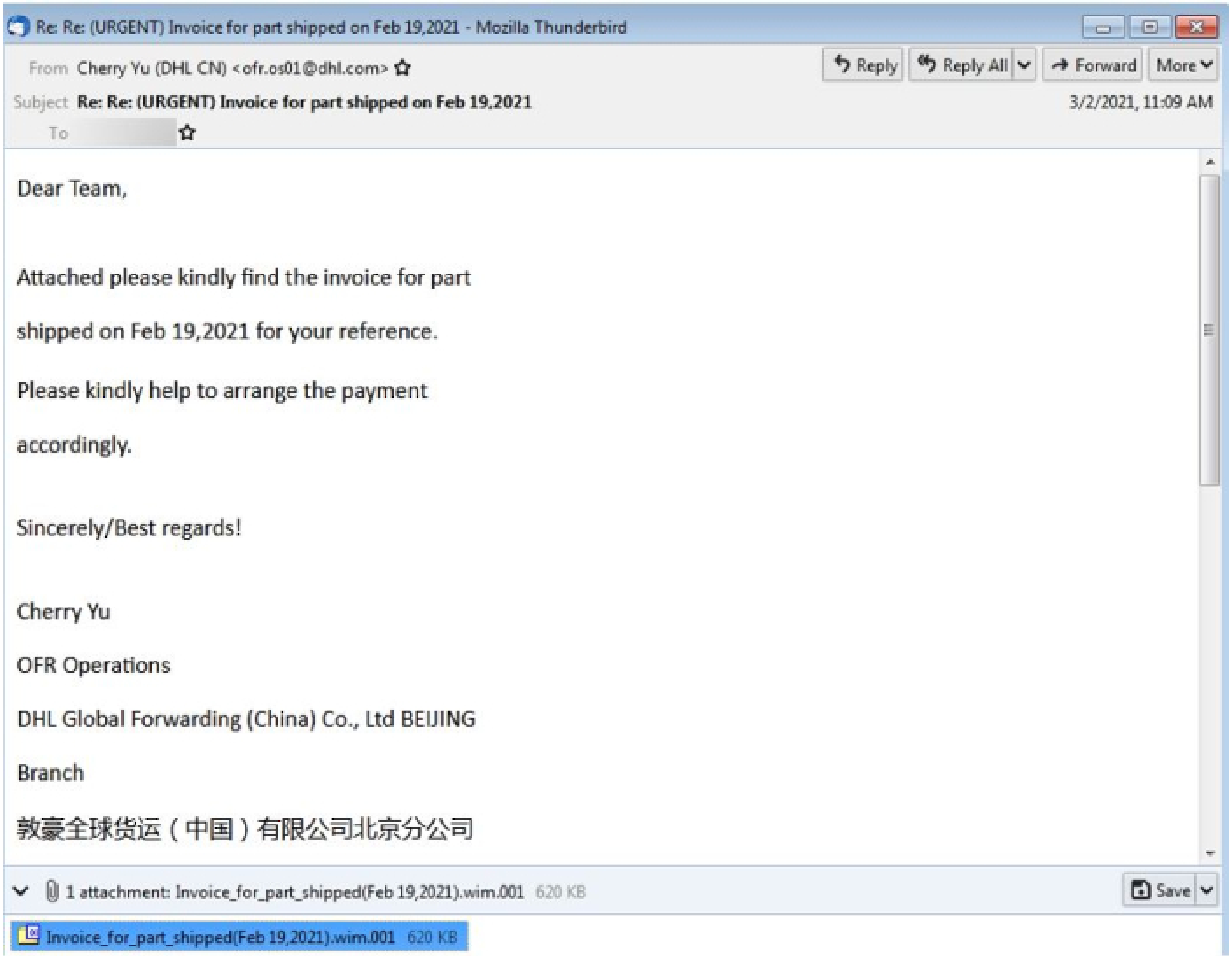
Yet Another Archive Format Smuggling Malware

trustwave.com/en-us/resources/blogs/spiderlabs-blog/another-archive-format-smuggling-malware/



The use of novel disk image files to encapsulate malware distributed via spam has been a theme that we have highlighted over the past couple of years. As anticipated, we have seen more disk image file formats being used, in addition to .ISO, .IMG, and .DAA which we blogged about.

We recently spotted another file format being used. These spams, spoofing courier companies, contain a malicious WIM (Windows Imaging Format) file disguised as an invoice or consignment note. WIM is a file-based disk image format developed by Microsoft. The file format serves to deploy Windows software components and updates ever since Windows Vista. This format uses a ".wim" extension and its content can be extracted using archiving tools like 7Zip, PowerISO, and PeaZip. Below are some samples from this campaign.



Re: Re: (URGENT) Invoice for part shipped on Feb 19,2021 - Mozilla Thunderbird
Reply
Reply All
Forward
More
Save

From Cherry Yu (DHL CN) <ofr.os01@dhl.com>

Subject Re: Re: (URGENT) Invoice for part shipped on Feb 19,2021

3/2/2021, 11:09 AM

To [redacted]

Dear Team,

Attached please kindly find the invoice for part

shipped on Feb 19,2021 for your reference.

Please kindly help to arrange the payment

accordingly.

Sincerely/Best regards!

Cherry Yu

OFR Operations

DHL Global Forwarding (China) Co., Ltd BEIJING

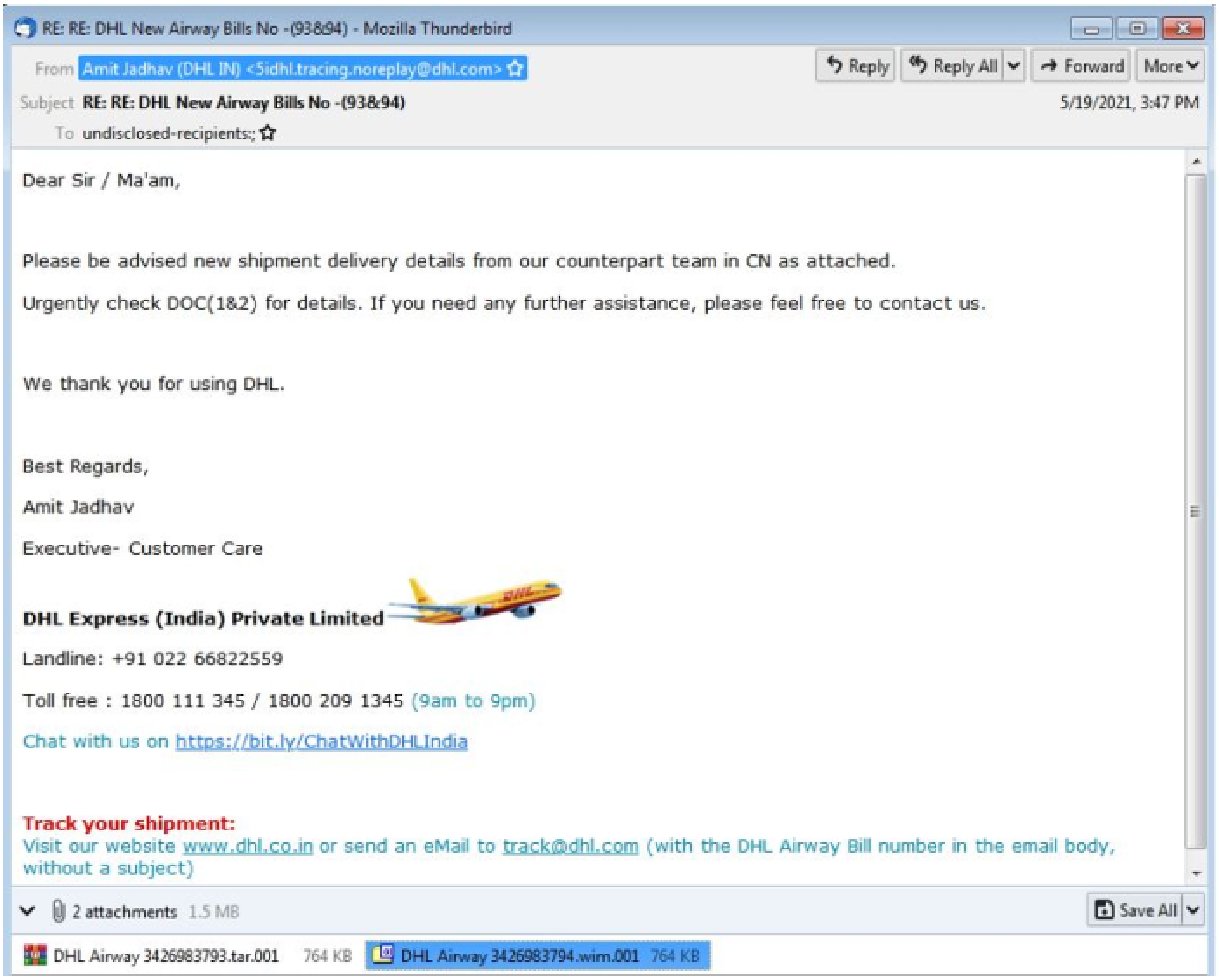
Branch

敦豪全球货运（中国）有限公司北京分公司

1 attachment: Invoice_for_part_shipped(Feb 19,2021).wim.001 620 KB

Invoice_for_part_shipped(Feb 19,2021).wim.001 620 KB

Figure 1: A DHL spam containing a fake invoice attachment



RE: RE: DHL New Airway Bills No -(93&94) - Mozilla Thunderbird
Reply
Reply All
Forward
More
Save All

From Amit Jadhav (DHL IN) <5idhl.tracing.noreplay@dhl.com>

Subject RE: RE: DHL New Airway Bills No -(93&94)

5/19/2021, 3:47 PM

To undisclosed-recipients;

Dear Sir / Ma'am,

Please be advised new shipment delivery details from our counterpart team in CN as attached.

Urgently check DOC(1&2) for details. If you need any further assistance, please feel free to contact us.

We thank you for using DHL.

Best Regards,

Amit Jadhav

Executive- Customer Care

DHL Express (India) Private Limited

Landline: +91 022 66822559

Toll free : 1800 111 345 / 1800 209 1345 (9am to 9pm)

Chat with us on https://bit.ly/ChatWithDHLIndia

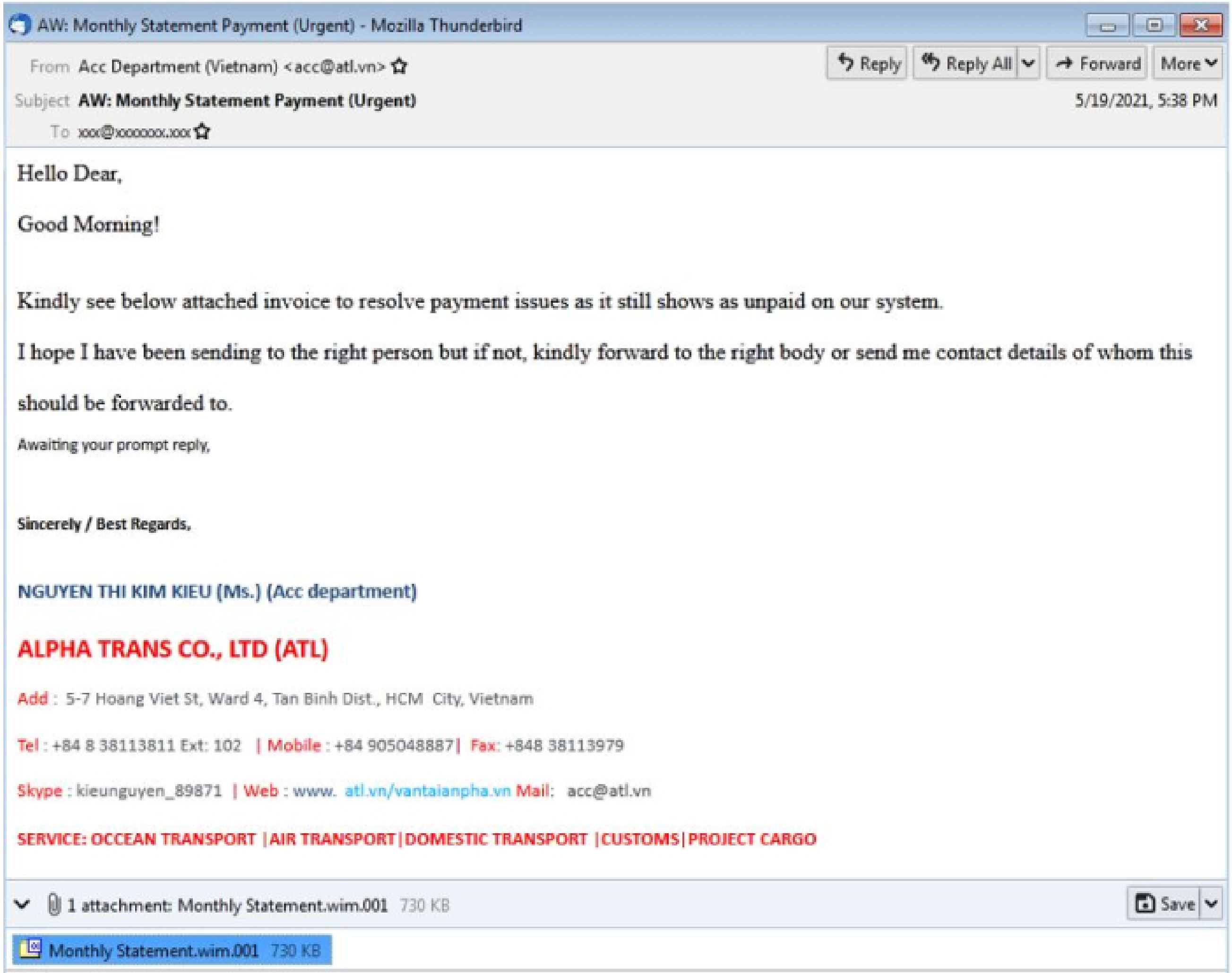
Track your shipment:
Visit our website www.dhl.co.in or send an eMail to track@dhl.com (with the DHL Airway Bill number in the email body, without a subject)

2 attachments 1.5 MB

DHL Airway 3426983793.tar.001 764 KB

DHL Airway 3426983794.wim.001 764 KB

***Figure 2**: A DHL spam containing multiple malicious attachments disguised as consignment documents*



AW: Monthly Statement Payment (Urgent) - Mozilla Thunderbird

From Acc Department (Vietnam) <acc@atl.vn>
Subject **AW: Monthly Statement Payment (Urgent)**
To xxx@xxxxxxx.xxx

5/19/2021, 5:38 PM

Hello Dear,

Good Morning!

Kindly see below attached invoice to resolve payment issues as it still shows as unpaid on our system.

I hope I have been sending to the right person but if not, kindly forward to the right body or send me contact details of whom this should be forwarded to.

Awaiting your prompt reply,

Sincerely / Best Regards,

NGUYEN THI KIM KIEU (Ms.) (Acc department)

ALPHA TRANS CO., LTD (ATL)

Add : 5-7 Hoang Viet St, Ward 4, Tan Binh Dist., HCM City, Vietnam

Tel : +84 8 38113811 Ext: 102 | Mobile : +84 905048887| Fax: +848 38113979

Skype : kieunguyen_89871 | Web : www. atl.vn/vantaianpha.vn Mail: acc@atl.vn

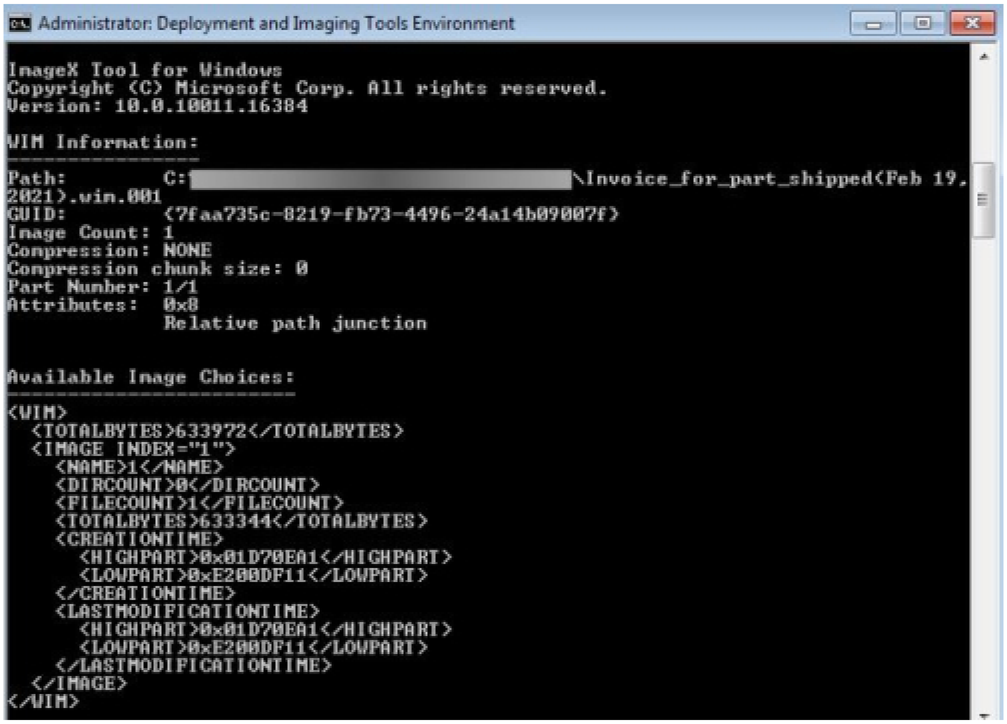
SERVICE: OCCEAN TRANSPORT |AIR TRANSPORT|DOMESTIC TRANSPORT |CUSTOMS|PROJECT CARGO

1 attachment: Monthly Statement.wim.001 730 KB

Monthly Statement.wim.001 730 KB

Figure 3: *A spam spoofing AlphaTrans containing a fake invoice attachment*

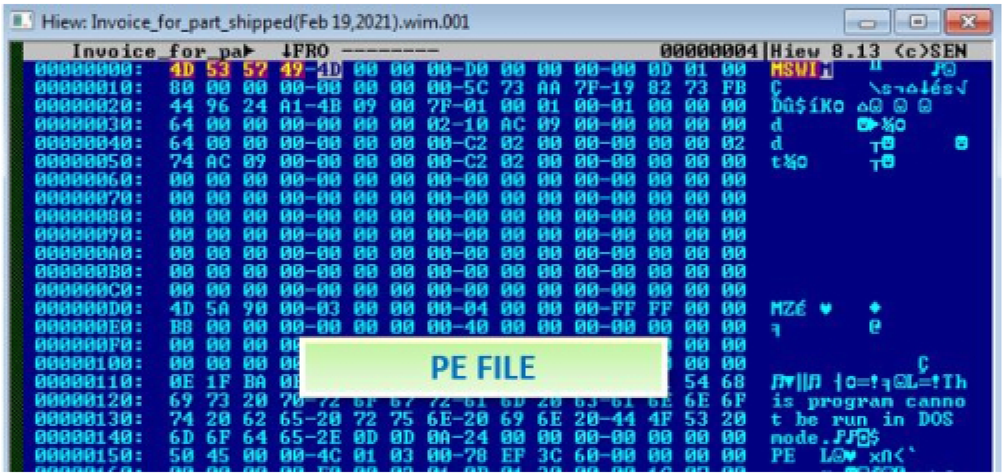
The attachments, although they have a ‘.wim.001’ file extension which denotes that they are the first part of a larger WIM file, have the complete file structure of a WIM file. Using the ImageX tool, we verified that all the WIM attachments we collected are not compressed and have one file only.



```
Administrator: Deployment and Imaging Tools Environment

ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Version: 10.0.10011.16384

WIM Information:
----------------
Path:        C:[redacted]\Invoice_for_part_shipped(Feb 19,
2021).wim.001
GUID:        {7faa735c-8219-fb73-4496-24a14b09007f}
Image Count: 1
Compression: NONE
Compression chunk size: 0
Part Number: 1/1
Attributes:  0x8
             Relative path junction


Available Image Choices:
------------------------
<WIM>
  <TOTALBYTES>633972</TOTALBYTES>
  <IMAGE INDEX="1">
    <NAME>1</NAME>
    <DIRCOUNT>0</DIRCOUNT>
    <FILECOUNT>1</FILECOUNT>
    <TOTALBYTES>633344</TOTALBYTES>
    <CREATIONTIME>
      <HIGHPART>0x01D70EA1</HIGHPART>
      <LOWPART>0xE200DF11</LOWPART>
    </CREATIONTIME>
    <LASTMODIFICATIONTIME>
      <HIGHPART>0x01D70EA1</HIGHPART>
      <LOWPART>0xE200DF11</LOWPART>
    </LASTMODIFICATIONTIME>
  </IMAGE>
</WIM>
```

Figure 4: *The information about the WIM attached in Fig. 1 using the tool ImageX*

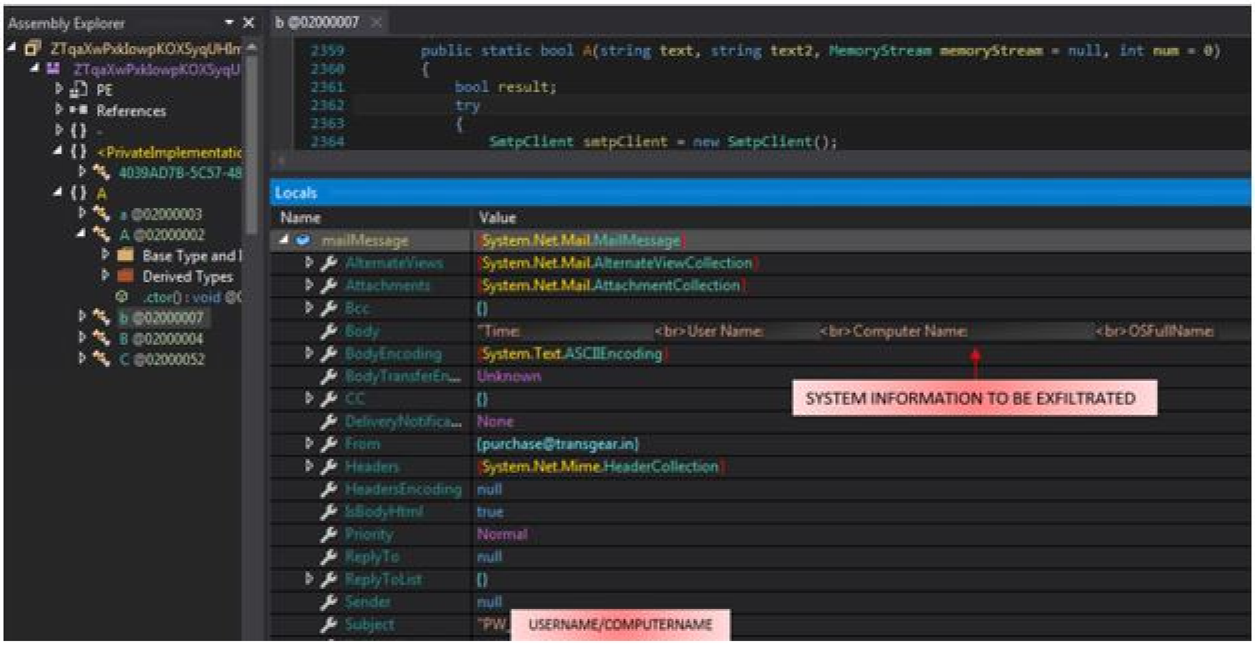
Opening the WIM files in a hex editor, its immediately noticeable that an executable file is hiding in them. Using the archiving tool 7Zip as displayed in Fig. 3, the EXE file bearing the same name as its WIM container can be extracted.



```
Hiew: Invoice_for_part_shipped(Feb 19,2021).wim.001
   Invoice_for_pa▸  ↓FRO ---------             00000004 |Hiew 8.13 (c)SEN
00000000:  4D 53 57 49-4D 00 00 00-D0 00 00 00-00 0D 01 00  MSWIM
00000010:  80 00 00 00-00 00 00 00-5C 73 AA 7F-19 82 73 FB  Ç       \s¬⌂↓és√
00000020:  44 96 24 A1-4B 09 00 7F-01 00 01 00-01 00 00 00  Dû$íKo ⌂☺ ☺ ☺
00000030:  64 00 00 00-00 00 00 02-10 AC 09 00-00 00 00 00  d       ☻►¼o
00000040:  64 00 00 00-00 00 00 00-C2 02 00 00-00 00 00 02  d       ┬☻     ☻
00000050:  74 AC 09 00-00 00 00 00-C2 02 00 00-00 00 00 00  t¼o     ┬☻
00000060:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000070:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000080:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000090:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000A0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000B0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000C0:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000D0:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  MZÉ ♥   ♦
000000E0:  B8 00 00 00-00 00 00 00-40 00 00 00-00 00 00 00  ╕       @
000000F0:  00 00 00 00                               00 00
00000100:  00 00 00 00                               00 00             Ç
00000110:  0E 1F BA 0E                               54 68  ♫▼║♫ ┤◘=!╕☺L=!Th
00000120:  69 73 20 70-72 6F 67 72-61 6D 20 63-61 6E 6E 6F  is program canno
00000130:  74 20 62 65-20 72 75 6E-20 69 6E 20-44 4F 53 20  t be run in DOS
00000140:  6D 6F 64 65-2E 0D 0D 0A-24 00 00 00-00 00 00 00  mode.♪♪◙$
00000150:  50 45 00 00-4C 01 03 00-78 EF 3C 60-00 00 00 00  PE  L☺♥ xn<`
```

Figure 5: *The WIM attachment shown in Fig. 1 viewed using the tool Hiew*

All the WIM files we gathered from our samples contain Agent Tesla malware. This threat is a Remote Access Trojan (RAT) written in .Net which can take full control over a compromised system and can exfiltrate data via HTTP, SMTP, FTP, and Telegram. In 2020, Agent Tesla was one of the predominant RATs and early this year, we reported that this malware is still actively getting distributed in spam emails.



```
public static bool A(string text, string text2, MemoryStream memoryStream = null, int num = 0)
{
    bool result;
    try
    {
        SmtpClient smtpClient = new SmtpClient();
```

```
Name                  Value
mailMessage           {System.Net.Mail.MailMessage}
  AlternateViews      {System.Net.Mail.AlternateViewCollection}
  Attachments         {System.Net.Mail.AttachmentCollection}
  Bcc                 {}
  Body                "Time: [redacted] <br>User Name: [redacted] <br>Computer Name: [redacted] <br>OSFullName:
  BodyEncoding        {System.Text.ASCIIEncoding}
  BodyTransferEn...   Unknown
  CC                  {}
  DeliveryNotifica... None
  From                {purchase@transgear.in}
  Headers             {System.Net.Mime.HeaderCollection}
  HeadersEncoding     null
  IsBodyHtml          true
  Priority            Normal
  ReplyTo             null
  ReplyToList         {}
  Sender              null
  Subject             "PW_
```

SYSTEM INFORMATION TO BE EXFILTRATED

USERNAME/COMPUTERNAME

***Figure 6**: The SMTP process of the Agent Tesla malware contained in Fig. 5 using DNSpy*

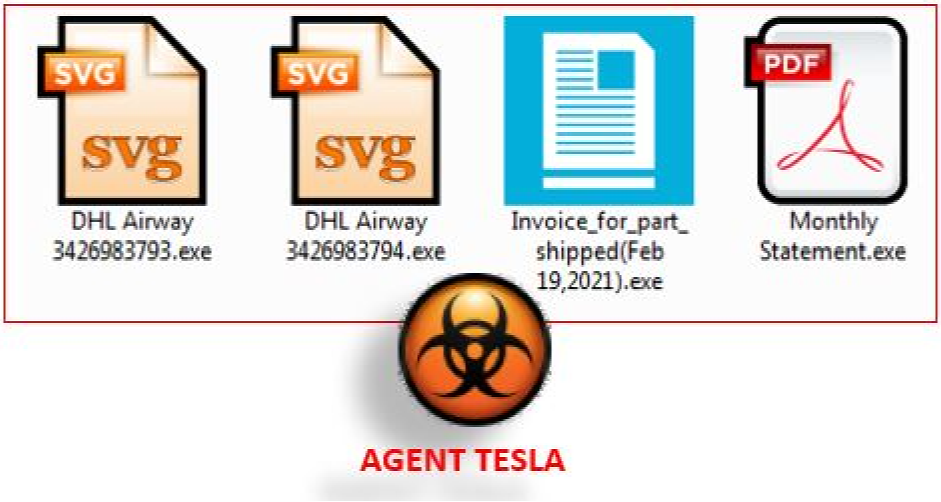

SVG
svg
DHL Airway 3426983793.exe
SVG
svg
DHL Airway 3426983794.exe
Invoice_for_part_shipped(Feb 19,2021).exe
PDF
Monthly Statement.exe
AGENT TESLA

***Figure 7**: The Agent Tesla malware extracted from the spam seen in this blog*

Summary

Encapsulating malware in an unusual archive file format is one of the common ways to bypass gateways and scanners. However, this strategy also poses a hurdle – the target system must recognize the file type or at least have a tool which can unpack and process the file. In contrast to the more popular .IMG and .ISO disk image files, WIM files are not supported by Windows built-in ability to mount disk image files. Moreover, the other popular archive utilities WinRAR and WinZip do not recognize the WIM disk image. WIM files can be processed with the widely used 7Zip.

In terms of suspiciousness, an inbound email containing a WIM file is not usual and should raise a few flags. Administrators could look to block these outright. Trustwave MailMarshal detects these threats bundled inside unusual disk imaging containers using a combination of its unpacking engine and its multi-layered threat detection technology.

IOC

WIM Files:
DHL Airway 3426983794.wim.001 (782102 bytes) SHA1: 91E3FE9AF48482484A4AAC9573D1FB13CB428738
Invoice_for_part_shipped(Feb 19,2021).wim.001 (634678 bytes) SHA1: D37C13A36A92114A927860B7021EB0C71BE73FBF
Monthly Statement.wim.001 (747278 bytes) SHA1: 2498342105E1C196C73960654E751D441925ED5C

Agent Tesla:
DHL Airway 3426983793.exe (780800 bytes) SHA1: 62FC617343B3D823362C8D9EA89AA676F79CE972
DHL Airway 3426983794.exe (780800 bytes) SHA1: 62FC617343B3D823362C8D9EA89AA676F79CE972
Invoice_for_part_shipped(Feb 19,2021).exe (633344 bytes) SHA1: F02FAFB08125D877584F73D5077DFCA95D66318C
Monthly Statement.exe (745984 bytes) SHA1: 236D1F71EB2EFA0C24E7EBA4390FEFE3691F1C68

Other:
DHL Airway 3426983793.tar.001 (782336 bytes) SHA1: E31107CCE2AA0DCF8B8C064EFEACAD5508C69D29