A QUICK DIVE INTO EMAIL FORENSICS

Anežka Lábusová

CONTENT

- Why this topic?
- What to look for
- Easy to use tools
- Real life examples

ABOUT ME

- Cybersecurity student at the University of Defence
- Gained experience as a part-time cybersecurity specialist at STYRAX, a.s.
- Active participant in various CTF events
- Open-source technologies enthusiast

WHY THIS TOPIC?

- Still a relevant topic
- You can share the things mentioned in this presentation and help raise awareness
- Or just take a look under the hood of spam emails in your inbox and have some fun analyzing them

WHAT TO LOOK FOR

- Headers
  - From, To, CC, BCC
  - Return-Path
  - Date/timestamps
  - X-Originating-IP / X-Mailer
- Body & content
- Attachments

EASY TO USE TOOLS

NOTEPAD

- Download the email (.eml file)
- Open it with notepad

EMLDUMP.PY

- From the creator of oledump.py, Didier Stevens
- Easy way to dump various parts of the email (plaintext, images, …)

```
anezk@linux-is-better MINGW64 ~/Downloads
$ python emldump.py spam.eml
1: M         multipart/alternative
2:      3162 text/plain
3:      4788 text/html

anezk@linux-is-better MINGW64 ~/Downloads
$ python emldump.py spam.eml -d -s 2
Dobr&#253; den
Tohle je posledn&#237; varov&#225;n&#237;.
V&#225;&#353; syst&#233;m byl hacknut.
V&#353;echna data byla zkop&#237;rov&#225;na z va&#353;eho za&#345;&#237;zen&#237; na na&#353;e servery.
Tak&#233; z fotoapar&#225;tu bylo nahr&#225;no video s va&#353;&#237; &#250;&#269;ast&#237; p&#345;i sledov&#225;n&#237; porna.
M&#367;j virus infikoval va&#353;e za&#345;&#237;zen&#237; prost&#345;ednictv&#237;m webu pro dosp&#283;l&#233;,kter&#233; jste ned&#225;vno nav&#353;t&#237;vili.
Jestli nev&#237;&#353;, jak to funguje, pod&#283;l&#237;m se o detaily.
Trojsk&#253; virus mi d&#225;v&#225; pln&#253; p&#345;&#237;stup a kontrolu nad za&#345;&#237;zen&#237;m, kter&#233; pou&#382;&#237;v&#225;te.
V d&#367;sledku toho vid&#237;m celou obrazovku, zap&#237;n&#225;m kameru a mikrofon a ani o tom nebudete v&#283;d&#283;t.
Zachytil jsem video z obrazovky a kamerov&#233;ho za&#345;&#237;zen&#237; a namontoval video, na kter&#233; je v jedn&#233; &#269;&#225;sti obrazovky video jako masturbujete, a v jin&#233;m pornografick&#233;m
videu, kter&#233; jste v tu chv&#237;li otev&#345;eli.
Vid&#237;m cel&#253; seznam va&#353;ich kontakt&#367; s va&#353;&#237;m telefonem a v&#353;emi soci&#225;ln&#237;mi s&#237;t&#283;mi.
V jednu chv&#237;li mohu toto video odeslat do cel&#233;ho seznamu va&#353;ich telefonn&#237;ch, po&#353;tovn&#237;ch a soci&#225;ln&#237;ch m&#233;di&#237;.
Krom&#283; toho mohu tak&#233; odeslat v&#353;echna data z va&#353;eho e-mailu i z posl&#367;.
M&#367;&#382;u ti nav&#382;dy zni&#269;it reputaci.
Pokud se chcete t&#283;mto d&#367;sledk&#367;m vyhnout, pak:
P&#345;ev&#225;d&#283;t $1000 (US$) do m&#233; bitcoinov&#233; pen&#283;&#382;enky
(pokud nev&#237;te, jak to ud&#283;lat, napi&#353;te na vyhled&#225;vac&#237; &#345;&#225;dek Google: &#8220;Koupit Bitcoin&#8221;).
Moje bitcoinov&#225; pen&#283;&#382;enka (PEN&#282;&#381;ENKA BTC): bc1qsfwe849m8ehj4zkekex8uqkvqhpg9v46f9hrcy
Jakmile doraz&#237; platba, okam&#382;it&#283; zni&#269;&#237;m va&#353;e video a zaru&#269;&#237;m, &#382;e v&#225;s nebudu obt&#283;&#382;ovat znovu.
Na tuto platbu m&#225;te 50 hodin (n&#283;co p&#345;es 2 dny).
Dostal jsem automatick&#233; ozn&#225;men&#237;, abych si p&#345;e&#269;etl tento dopis.Podobn&#283; &#268;asova&#269; se automaticky p&#345;epne po p&#345;e&#269;ten&#237; aktu&#225;ln&#237; zpr&#225;vy.
Nepokou&#353;ejte se nikde st&#283;&#382;ovat, proto&#382;e pen&#283;&#382;enka nem&#367;&#382;e sledovat, po&#353;ta, odkud dopis poch&#225;z&#237;, tak&#233; nen&#237; sledov&#225;na a vytvo&#345;ena automaticky, tak&#382;e pro m&#283; nem&#225; smysl ps&#225;t.
Pokud se pokus&#237;te tento e-mail s n&#283;k&#253;m sd&#237;let, syst&#233;m automaticky ode&#353;le po&#382;adavek na servery a za&#269;nou odes&#237;lat v&#353;echna data na soci&#225;ln&#237; s&#237;t&#283;;.
zm&#283;na hesel na soci&#225;ln&#237;ch s&#237;t&#237;ch, na po&#353;t&#283;, v za&#345;&#237;zen&#237; v&#225;m nepom&#367;&#382;e, proto&#382;e v&#353;echna data ji&#382; byla sta&#382;ena do clusteru m&#253;ch server&#367;.
Hodn&#283; &#353;t&#283;st&#237; a neumo&#382; nic hloup&#233;ho. Mysli na svou reputaci.
anezk@linux-is-better MINGW64 ~/Downloads
$
```

MINGW64:/c/Users/anezk/Downloads

```
anezk@linux-is-better MINGW64 ~/Downloads
$ python emldump.py pics.eml
1: M         multipart/mixed
2:        233 text/plain
3:    2720001 image/jpeg (20250520_103738.jpg)
4:    2689028 image/jpeg (20250520_104124.jpg)

anezk@linux-is-better MINGW64 ~/Downloads
$ python emldump.py pics.eml -d -s 3 > image.jpg

anezk@linux-is-better MINGW64 ~/Downloads
$
```

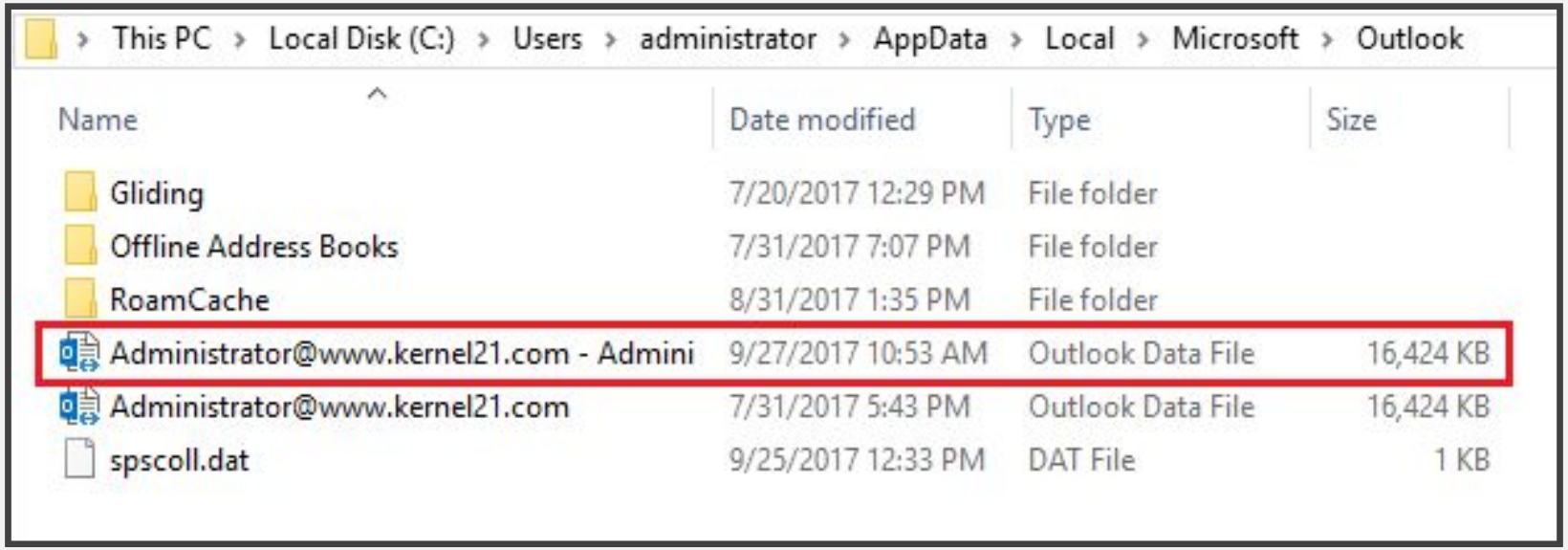
Upravit

image.jpg

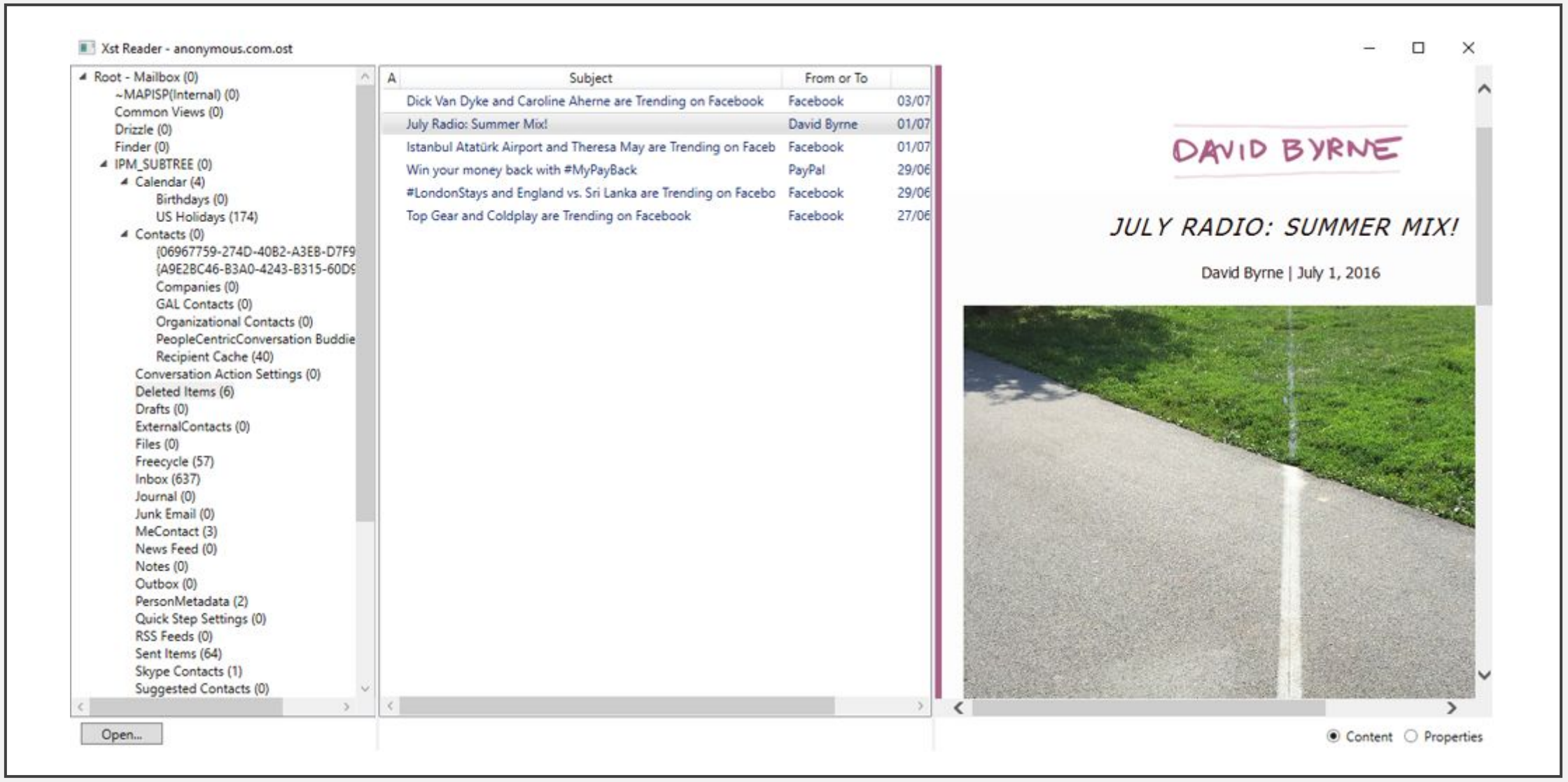
24 %

XST READER

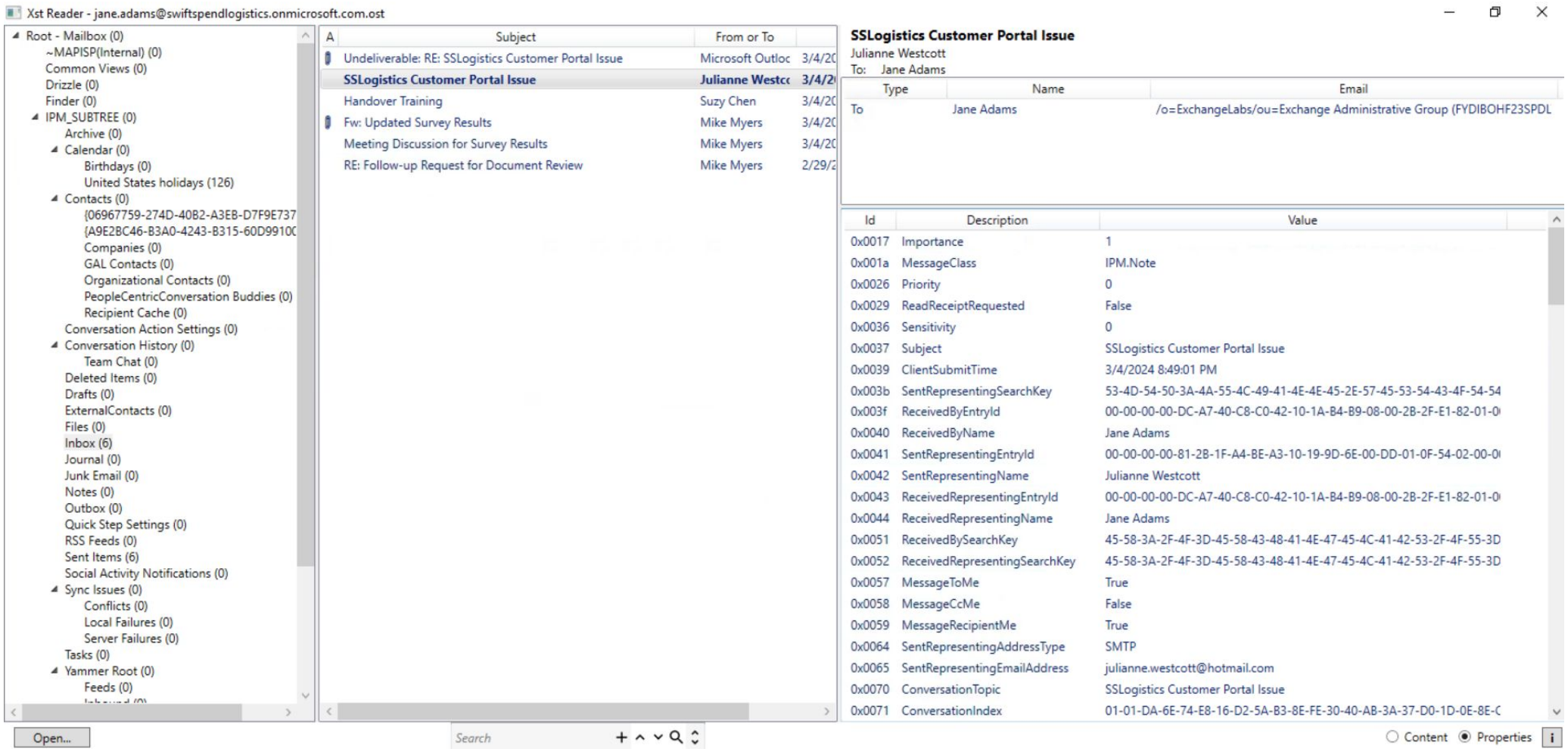
- GUI tool for viewing MS Outlook's .ost and .pst files
- You can find the .ost file here:



Source:
www.stellarinfo.com



Source:
https://github.com/Dijji/XstReader/blob/master/screenshot5.png



Source:
https://tryhackme.com/room/windowsapplications

AUTOPSY

- Email parser modules
- Correlating with other evidence on a disk

REAL LIFE EXAMPLES

FIRST EXAMPLE

- Found a spam email in my spam folder
- Without subject
- I saw only the display name of the sender and not the full address
- In a preview I saw a part of the message saying „Hello, this is the last warning…“

WHAT I FOUND OUT

- IP address of the sender
  - Located in Bangladesh
- Date and time
  - Different time zones
- Email address of the sender
- User-Agent
  - Email client from year 2009
- Email content

```
Received: from [203.223.89.55] ([203.223.89.54])
        by smtpd-mx-5584f548dd-pn4sg (szn-email-smtpd/2.0.60) with ESMTP
        id 2d2ec201-3ddb-4b65-a2bd-1733820756de;
        Fri, 01 Aug 2025 13:23:52 +0200
Message-ID: <688CF81B.6060400@dkv.lbc.cd.cz>
Date: Fri, 01 Aug 2025 22:23:39 +0500
From: "reggie joni" <hanus@dkv.lbc.cd.cz>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9pre) Gecko/2008050715 Thunderbird/3.0a1
MIME-Version: 1.0
To: <[redacted]@seznam.cz>
Subject:
Content-Type: multipart/alternative;
 boundary="------------000605090407030203010306"

This is a multi-part message in MIME format.
--------------000605090407030203010306
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: quoted-printable

Dobr&#253; den
Tohle je posledn&#237; varov&#225;n&#237;.
V&#225;&#353; syst&#233;m byl hacknut.
V&#353;echna data byla zkop&#237;rov&#225;na z va&#353;eho =
za&#345;&#237;zen&#237; na na&#353;e servery.
Tak&#233; z fotoapar&#225;tu bylo nahr&#225;no video s va&#353;&#237; =
&#250;&#269;ast&#237; p&#345;i sledov&#225;n&#237; porna.
M&#367;j virus infikoval va&#353;e za&#345;&#237;zen&#237; =
prost&#345;ednictv&#237;m webu pro dosp&#283;l&#233;,kter&#233; jste =
ned&#225;vno nav&#353;t&#237;vili.
Jestli nev&#237;&#353;, jak to funguje, pod&#283;l&#237;m se o detaily.
Trojsk&#253; virus mi d&#225;v&#225; pln&#253; p&#345;&#237;stup a =
kontrolu nad za&#345;&#237;zen&#237;m, kter&#233; =
pou&#382;&#237;v&#225;te.
V d&#367;sledku toho vid&#237;m celou obrazovku, zap&#237;n&#225;m =
kameru a mikrofon a ani o tom nebudete v&#283;d&#283;t.
Zachytil jsem video z obrazovky a kamerov&#233;ho =
za&#345;&#237;zen&#237; a namontoval video, na kter&#233; je v =
jedn&#233; &#269;&#225;sti obrazovky video jako masturbujete, a v =
jin&#233;m pornografick&#233;m videu, kter&#233; jste v tu chv&#237;li =
otev&#345;eli.
Vid&#237;m cel&#253; seznam va&#353;ich kontakt&#367; s va&#353;&#237;m =
telefonem a v&#353;emi soci&#225;ln&#237;mi s&#237;t&#283;mi.
V jednu chv&#237;li mohu toto video odeslat do cel&#233;ho seznamu =
va&#353;ich telefonn&#237;ch, po&#353;tovn&#237;ch a =
soci&#225;ln&#237;ch m&#233;di&#237;.
Krom&#283; toho mohu tak&#233; odeslat v&#353;echna data z va&#353;eho =
e-mailu i z posl&#367;.
M&#367;&#382;u ti nav&#382;dy zni&#269;it reputaci.
```

SECOND EXAMPLE

- Found a spam email in my spam folder
- With subject in Korean
- Spoofed my email address

WHAT I FOUND OUT

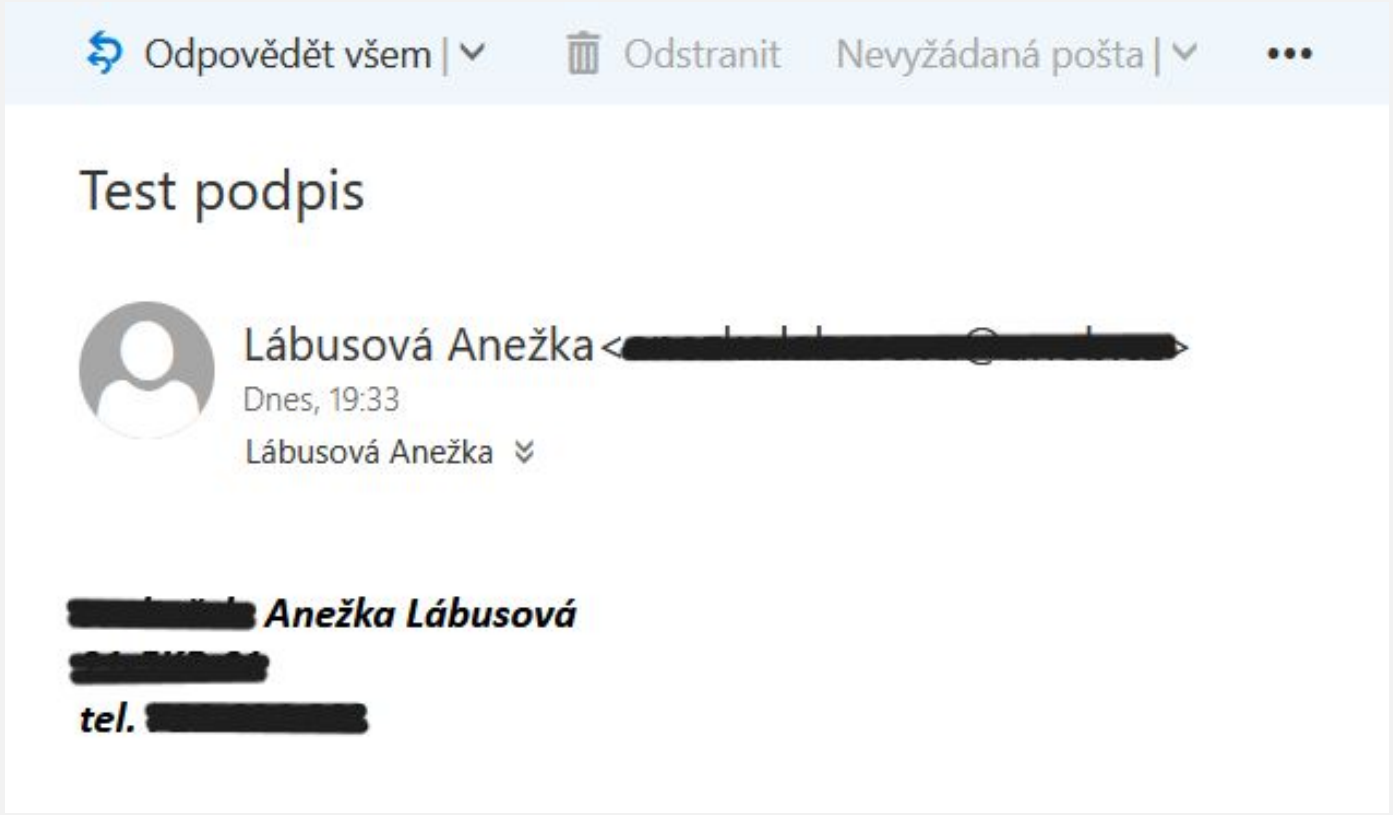
- IP address of the sender
  - Located in Mexico
- Date and time
  - Different time zones
- Proof of spoofing
- Content

```
Received: from customer-                    .cablevision.net.mx
        (customer-                  .cablevision.net.mx [                ])
        by smtpd-mx-5584f548dd-pn4sg (szn-email-smtpd/2.0.60) with ESMTP
        id 74679f71-e5f9-480e-a194-9dd0c88c073b;
        Thu, 31 Jul 2025 07:16:02 +0200
Message-ID: <5CAECFA0223DC14DBFDEB1332CD05CAE@GPOBLQJK>
From: <                @email.cz>
To: <                @email.cz>
Subject: =?utf-8?B?7ZiR66ClIOygnOyViA==?=
Date: 30 Jul 2025 18:09:56 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_002E_01DC01B0.07C103DA"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.1631
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.1631

This is a multi-part message in MIME format.

------=_NextPart_000_002E_01DC01B0.07C103DA
Content-Type: text/plain;
        charset="shift_jis"
Content-Transfer-Encoding: quoted-printable

&#50504;&#45397;&#54616;&#49464;&#50836;!
&#48372;&#49884;&#45796;&#49884;&#54588;, &#54644;&#45817; =
&#47700;&#51068;&#51008; &#44277;&#49885;&#51201;&#51060;&#51648; =
&#50506;&#51004;&#47728;, &#48520;&#54665;&#55176;&#46020;, =
&#50668;&#47084;&#48516;&#50640;&#44172; &#51339;&#51008; =
&#51032;&#48120;&#44032; &#50500;&#45785;&#45768;&#45796;.
&#54616;&#51648;&#47564; &#51208;&#47581;&#54616;&#51648; =
&#47560;&#49464;&#50836;, &#53356;&#44172; =
&#47928;&#51228;&#46104;&#51652; &#50506;&#49845;&#45768;&#45796;. =
&#51648;&#44552; &#47784;&#46304; &#49324;&#54637;&#50640; =
&#45824;&#54644;&#49436; =
&#49444;&#47749;&#54644;&#46300;&#47532;&#44192;&#49845;&#45768;&#45796;.=


&#51200;&#45716; &#44480;&#54616;&#44032; =
&#51221;&#44592;&#51201;&#51004;&#47196; =
&#49324;&#50857;&#54616;&#45716; &#47196;&#52972; =
&#45348;&#53944;&#50892;&#53356;&#51032; &#51204;&#51088; =
&#51109;&#52824;&#46308;&#50640; &#50529;&#49464;&#49828;&#54624; =
&#49688; &#51080;&#50632;&#49845;&#45768;&#45796;.
&#51648;&#45212; &#47751; &#45804; &#46041;&#50504; =
&#45817;&#49888;&#51032; &#54876;&#46041;&#51012; =
&#52628;&#51201;&#54616;&#50688;&#49845;&#45768;&#45796;.

&#50612;&#51788;&#45796; &#44536;&#47088; &#51068;&#51060; =
```

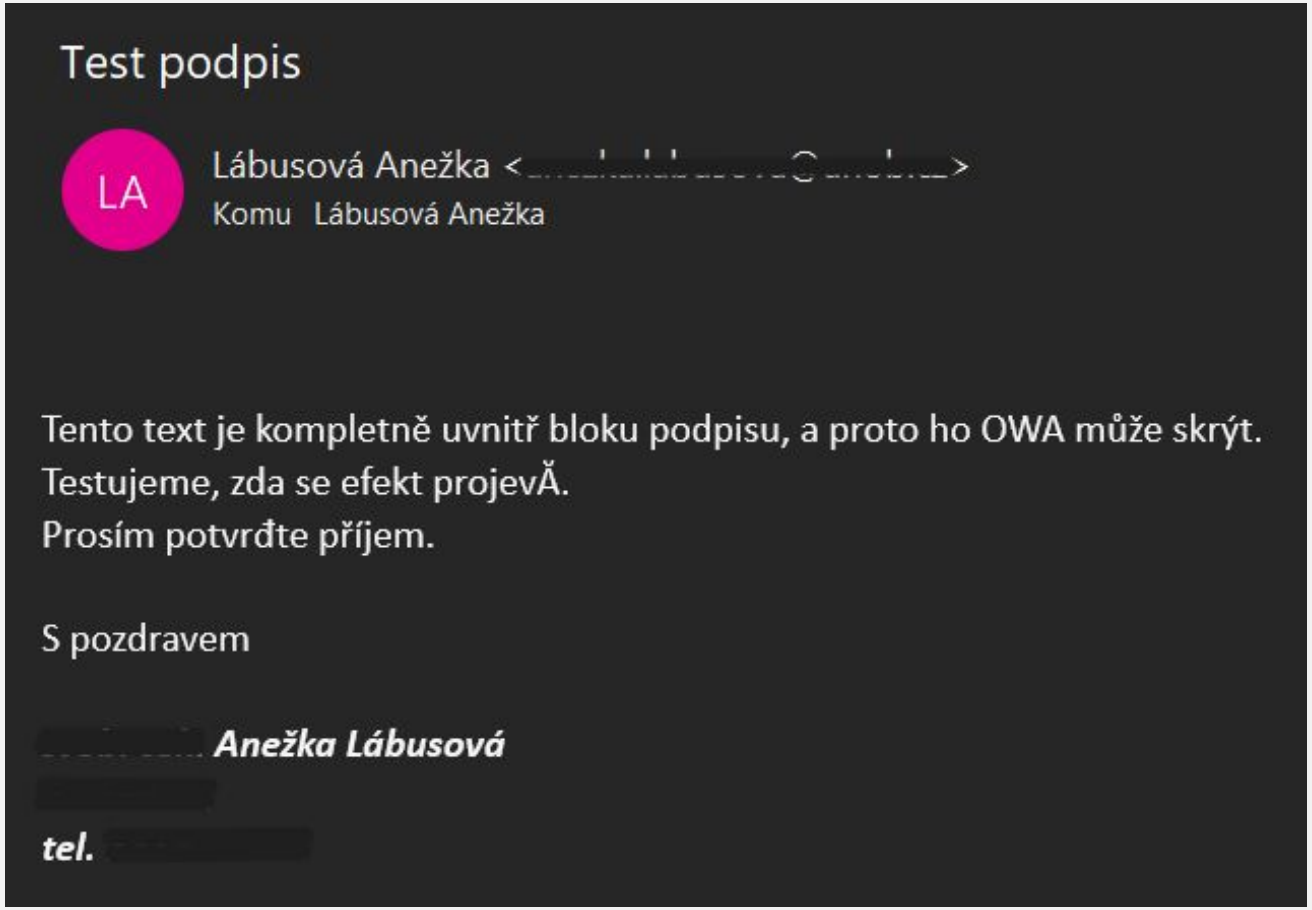
THIRD EXAMPLE

- I once sent an email to one of my teachers
- Only automatic signature was left after they received it

THIS IS HOW OUTLOOK WEB APP RENDERED IT



THIS IS HOW OUTLOOK DESKTOP APP/THUNDERBIRD RENDERED IT



WHAT HAPPENED?

- The message got into div block for signature and that resulted in bad HTML rendering in OWA

```
Content-Type: text/html; charset="iso-8859-2"
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Diso-8859-2">
<style type=3D"text/css" style=3D"display:none;"><!-- P {margin-top:0;margi=
n-bottom:0;} --></style>
</head>
<body dir=3D"ltr">
<div id=3D"divtagdefaultwrapper" style=3D"font-size: 12pt; color: rgb(0, 0,=
 0); font-family: Calibri, Helvetica, sans-serif;">
<p></p>
<div id=3D"Signature"><style type=3D"text/css" style=3D"display:none"> <!--=
 p  {margin-top:0;  margin-bottom:0} -</style>
Dobr=FD den,<br><br>
Tento text je kompletn=EC uvnit=F8 bloku podpisu, a proto ho OWA m=F9=BEe skr=FDt.<br>
Testujeme, zda se efekt projeví.<br>
Pros=EDm potvr=F0te p=F8=EDjem.<br><br>
S pozdravem
</div>
<div><br></div>
<div id=3D"Signature">
<style type=3D"text/css" style=3D"display:none"> <!-- p  {margin-top:0;  margin-bottom:0} --> </style>
<div dir=3D"ltr" style=3D"font-size:12pt; color:#000000; font-family:Calibri,Helvetica,sans-serif">
<p align=3D"left"><i><b>[redacted]. Ane=BEka L=E1busov=E1</b></i></p>
<p align=3D"left"><b><i>[redacted]</i></b></p>
<p align=3D"left"><i><b>tel. [redacted]</b></i></p>
</div>
</div>
</div>
</body>
</html>
```

Message

Signature

THANK YOU FOR YOUR ATTENTION
QUESTIONS?