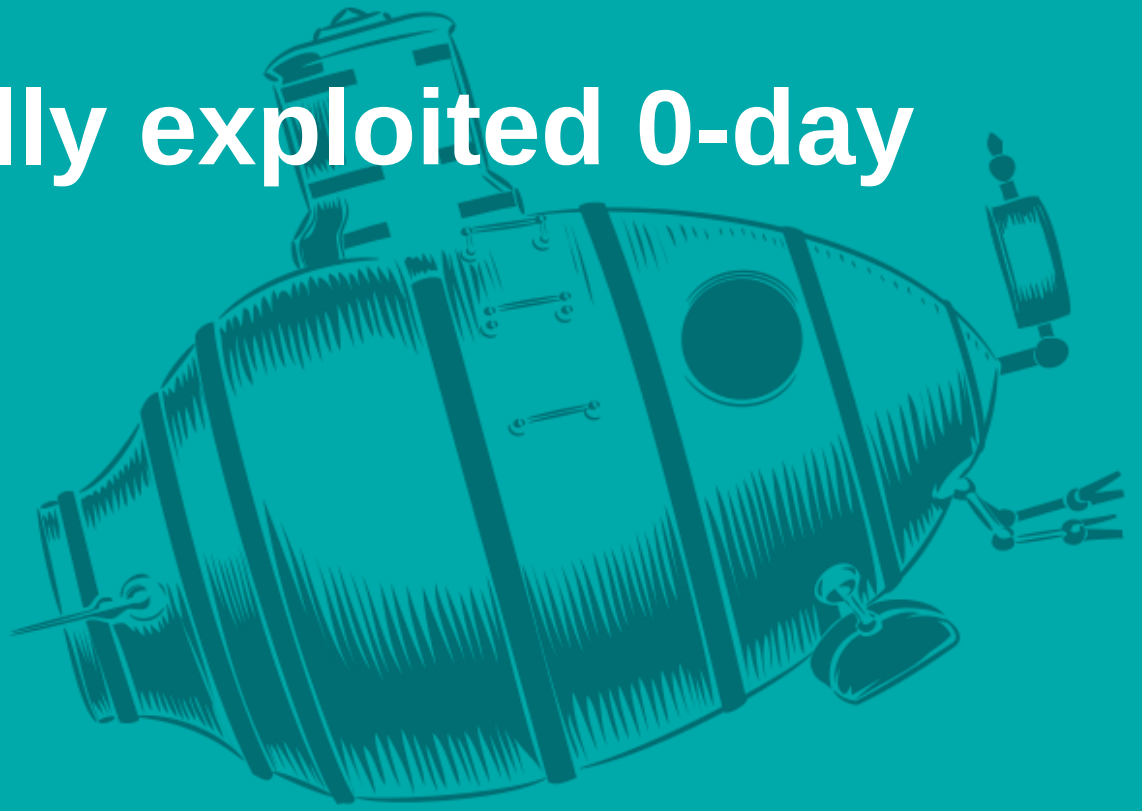
ALEF

The story of accidentally exploited 0-day in Outlook

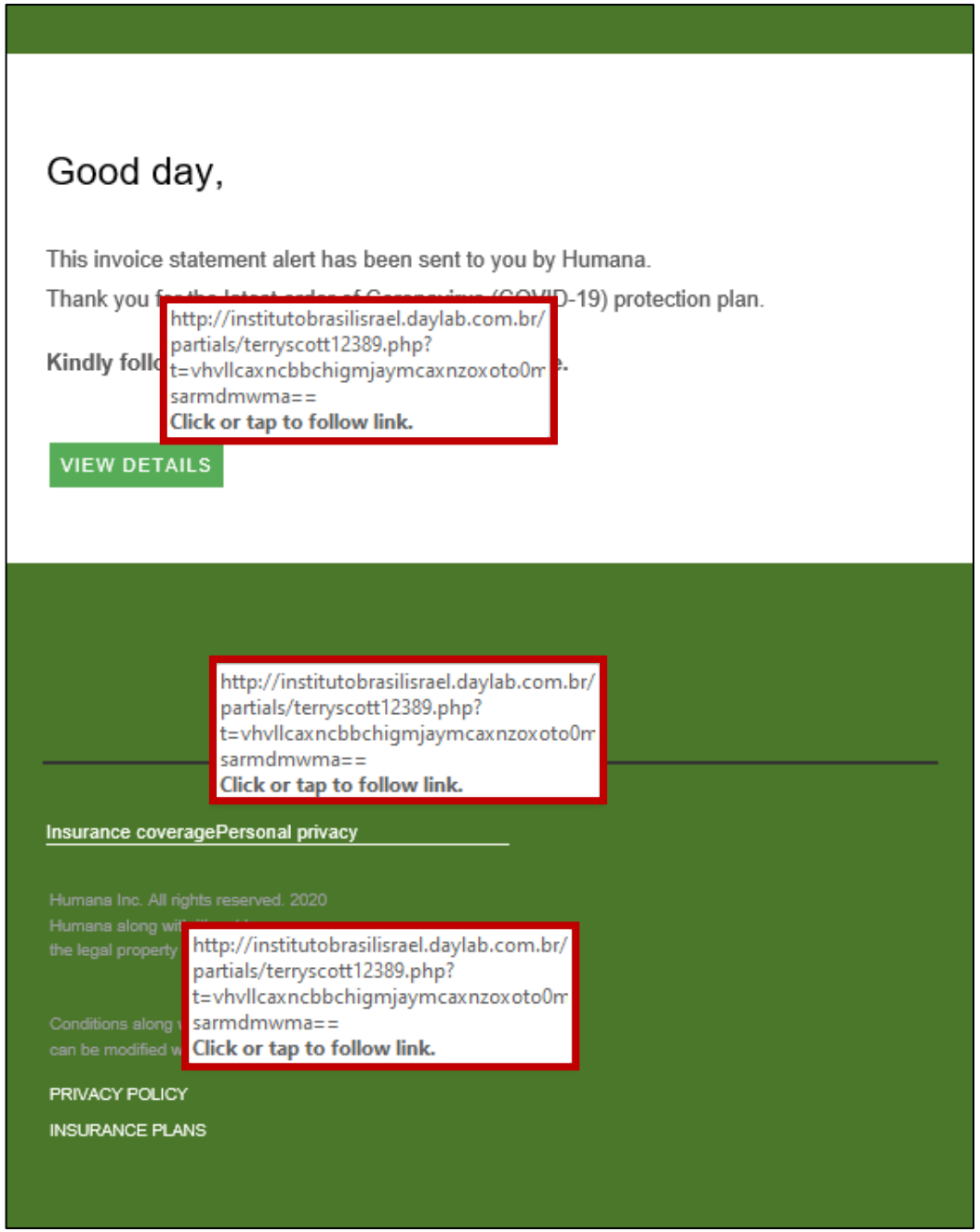


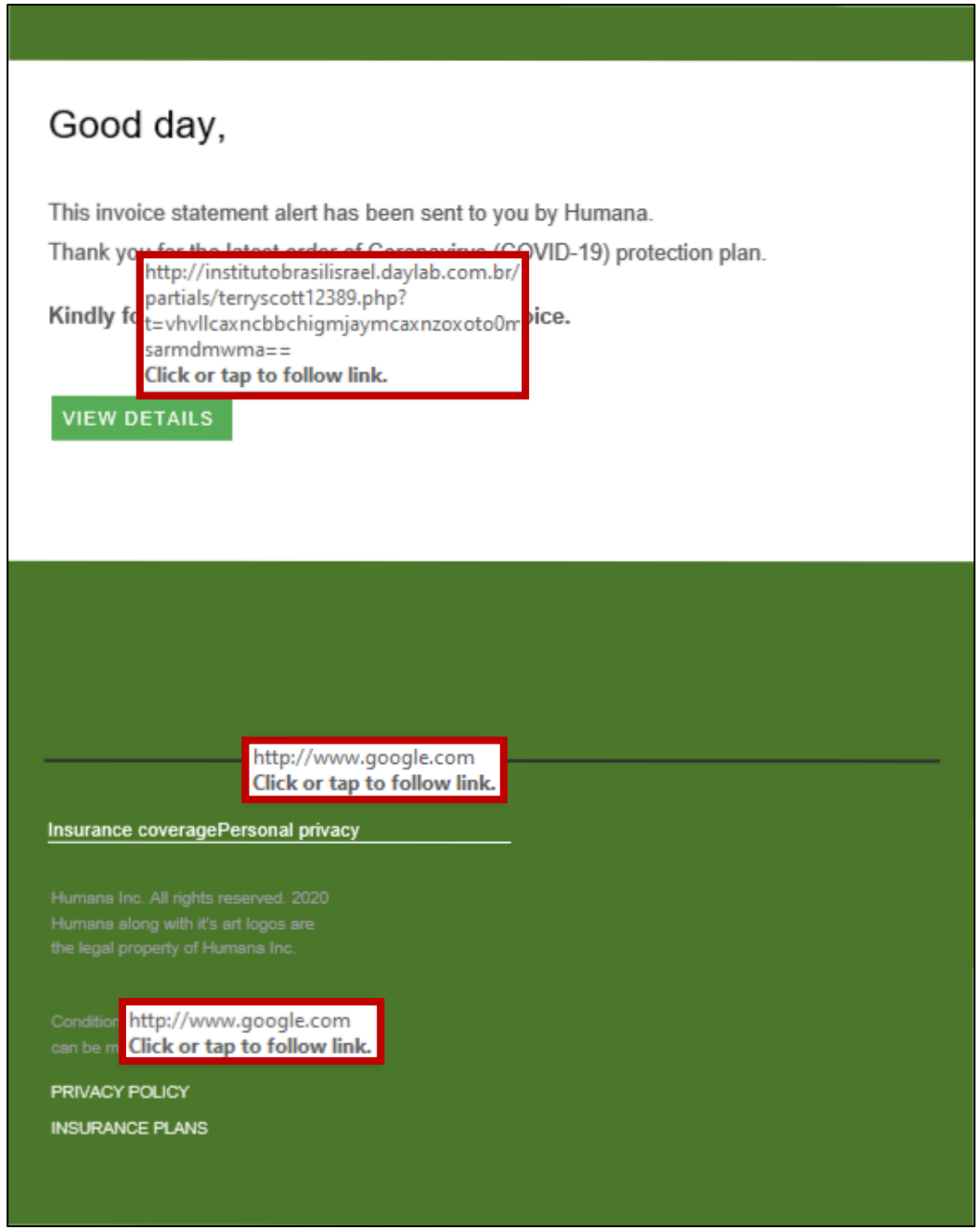
Jan Kopřiva

jan.kopriva@alef.com @jk0pr

ALEF CSIRT

TLP: WHITE


Good day,
This invoice statement alert has been sent to you by Humana.
Thank you
-19) protection plan.
Kindly follo
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=vhvllcaxncbbchigmjaymcaxnzoxoto0m
sarmdmwma==
Click or tap to follow link.
VIEW DETAILS
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=vhvllcaxncbbchigmjaymcaxnzoxoto0m
sarmdmwma==
Click or tap to follow link.
Insurance coveragePersonal privacy
Humana Inc. All rights reserved. 2020
Humana along wit
the legal property
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=vhvllcaxncbbchigmjaymcaxnzoxoto0m
sarmdmwma==
Click or tap to follow link.
Conditions along
can be modified
PRIVACY POLICY
INSURANCE PLANS


Good day,
This invoice statement alert has been sent to you by Humana.
Thank yo
VID-19) protection plan.
Kindly fo
ice.
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=vhvllcaxncbbchigmjaymcaxnzoxoto0m
sarmdmwma==
Click or tap to follow link.
VIEW DETAILS
http://www.google.com
Click or tap to follow link.
Insurance coveragePersonal privacy
Humana Inc. All rights reserved. 2020
Humana along with it's art logos are
the legal property of Humana Inc.
Condition
can be m
http://www.google.com
Click or tap to follow link.
PRIVACY POLICY
INSURANCE PLANS

ALEF

```
   <div> <span style="color: rgb(157, 157, 163); font-family: &quot;ClanPro-Medium&quot;,
Helvetica, Arial, sans-serif; font-size: 12px; line-height: 18px; display: inline-block;
padding-bottom: 4px">Humana Inc. All rights reserved. 2020 Humana along with it's art logos are
the legal property of Humana Inc.</span> <br> </div><br>        <span><br>Conditions along with
certain services can be modified without notification.</span>          </td> </tr>     <tr> <td
style="color: rgb(157, 157, 163); font-family: &quot;ClanPro-Medium&quot;, Helvetica, Arial,
sans-serif; font-size: 12px; line-height: 26px; padding-top: 6px; text-align: left" align="left">
<a href="http://www.google.com" style="color: rgb(255, 255, 255); text-decoration: none" target=
"_blank">PRIVACY POLICY </a> <br> <a href="http://www.google.com" style="color: rgb(255,
255, 255); text-decoration: none" target=" blank">INSURANCE PLANS</a></td> </tr>
</tbody></table></td> </tr> </tbody></table></td> </tr> </tbody></table>  </td> </tr>
</tbody></table></td> </tr> <tr> <td style="font-size: 0px; line-height: 0px; padding-top: 60px;
text-align: left"> </td> </tr> </tbody></table>  </td> </tr> </tbody></table></td> </tr>
</tbody></table></td> </tr> </tbody></table>   </td> </tr> </tbody></table>  </td> </tr> </tbody>
</table>  </td> </tr> </tbody> </table>   <img src="" alt="" width="1" height="1" border="0" style
="height: 1px !important; width: 1px !important; border-width: 0 !important; margin-top: 0
!important; margin-bottom: 0 !important; margin-right: 0 !important; margin-left: 0 !important;
padding-top: 0 !important; padding-bottom: 0 !important; padding-right: 0 !important;
padding-left: 0 !important">   </div></div>
```

'font-size:9.0pt;font-family:"Helvetica",sans-serif;color:#9D9DA3'><a href="
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=VHVlLCAxNCBBcHIgMjAyMCAxN
zoxOTo0MSArMDMwMA==" target="_blank">Humana Inc.
All rights reserved. 2020 Humana along with it's art logos are the legal property of Humana Inc.
<o:p></o:p> <span style=
'font-size:9.0pt;font-family:"Helvetica",sans-serif;color:#9D9DA3'><a href="
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=VHVlLCAxNCBBcHIgMjAyMCAxN
zoxOTo0MSArMDMwMA==" target="_blank">

Conditions along with certain services can be modified without notification.
<o:p></o:p>
 </td></tr><tr><td style='padding:4.5pt 0cm 0cm 0cm'><p class=MsoNormal style
='line-height:19.5pt'><span style=
'font-size:9.0pt;font-family:"Helvetica",sans-serif;color:#9D9DA3'><a href="
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=VHVlLCAxNCBBcHIgMjAyMCAxN
zoxOTo0MSArMDMwMA==" target="_blank"><span style=
'color:white'>PRIVACY POLICY
INSURANCE PLANS
<o:p></o:p>
 </td></tr></table></td></tr></table></td></tr></table></td></tr></table></td>

How did this happen?

ALEF

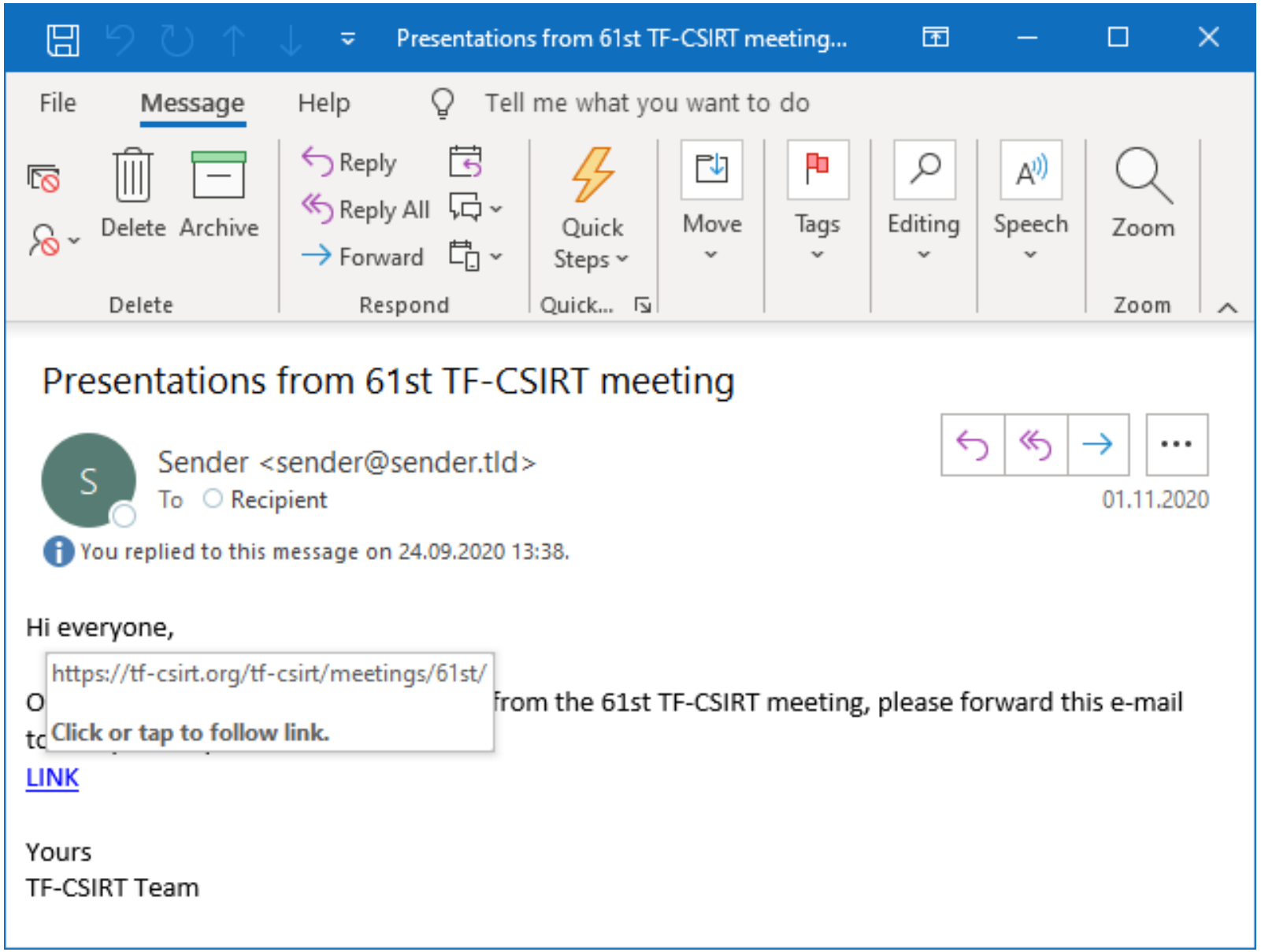
```
<a href="
http://institutobrasilisrael.daylab.com.br/partials/terryscott12389.php?t=VHVlLCAxNCBBcHIgMjAyMCAxNzoxOTo0MSArMDMwMA==" style="background-color: rgb(87, 173, 87); border-color: rgb(87, 173, 87); border-radius: 0px; border-style: solid; border-width: 13px 16px; color: rgb(255, 255, 255); display: inline-block; letter-spacing: 1px; max-width: 300px; min-width: 150px; text-align: center; text-decoration: none; text-transform: uppercase; text-align: left" target="_blank"> <span
 style="float: left; text-align: left">View Details</span>
<span style="float: right; padding-top: 2px; display: inline-block"> <img src="" width="16" height
="12" style="Margin-left: 16px; border: none; clear: both; display: block; margin-top: 2px;
max-width: 100%; outline: none; text-decoration: none; width: auto" alt=""></span>   </a>
```

What is the impact?

- Original sender can cause links to be changed/added when the message is forwarded

```
<html>
<body>
Hi everyone,<br><br>
On the following link are presentations from the 61st
TF-CSIRT meeting, please forward this e-mail to
everyone in your team.<br>
<a href="https://untrustednetwork.net/"><img></a>
<a href="https://tf-csirt.org/tf-csirt/meetings/61st/">
LINK</a>
<br><br>
Yours<br>
TF-CSIRT Team
</body>
</html>
```

ALEF


Presentations from 61st TF-CSIRT meeting...
File
Message
Help
Tell me what you want to do
Reply
Reply All
Forward
Delete
Archive
Quick Steps
Move
Tags
Editing
Speech
Zoom
Delete
Respond
Quick...
Zoom
Presentations from 61st TF-CSIRT meeting
S
Sender <sender@sender.tld>
To Recipient
01.11.2020
You replied to this message on 24.09.2020 13:38.
Hi everyone,
https://tf-csirt.org/tf-csirt/meetings/61st/
Click or tap to follow link.
from the 61st TF-CSIRT meeting, please forward this e-mail
LINK
Yours
TF-CSIRT Team

ALEF

RE: Presentations from 61st TF-CSIRT meeting

Jan Kopriva
To Jan Kopriva

13:38

FYI

From: Sender <sender@sender.tld>
Sent: Sunday, November 1, 2020 10:30 AM
To: Recipient <recipient@target.tld>
Subject: Presentations from 61st TF-CSIRT meeting

Hi everyone,

On the following link are presentations from the 61st TF-CSIRT meeting, please forward this e-mail to everyone in your team.

LINK https://untrustednetwork.net/
Click or tap to follow link.

Yours
TF-CSIRT Team

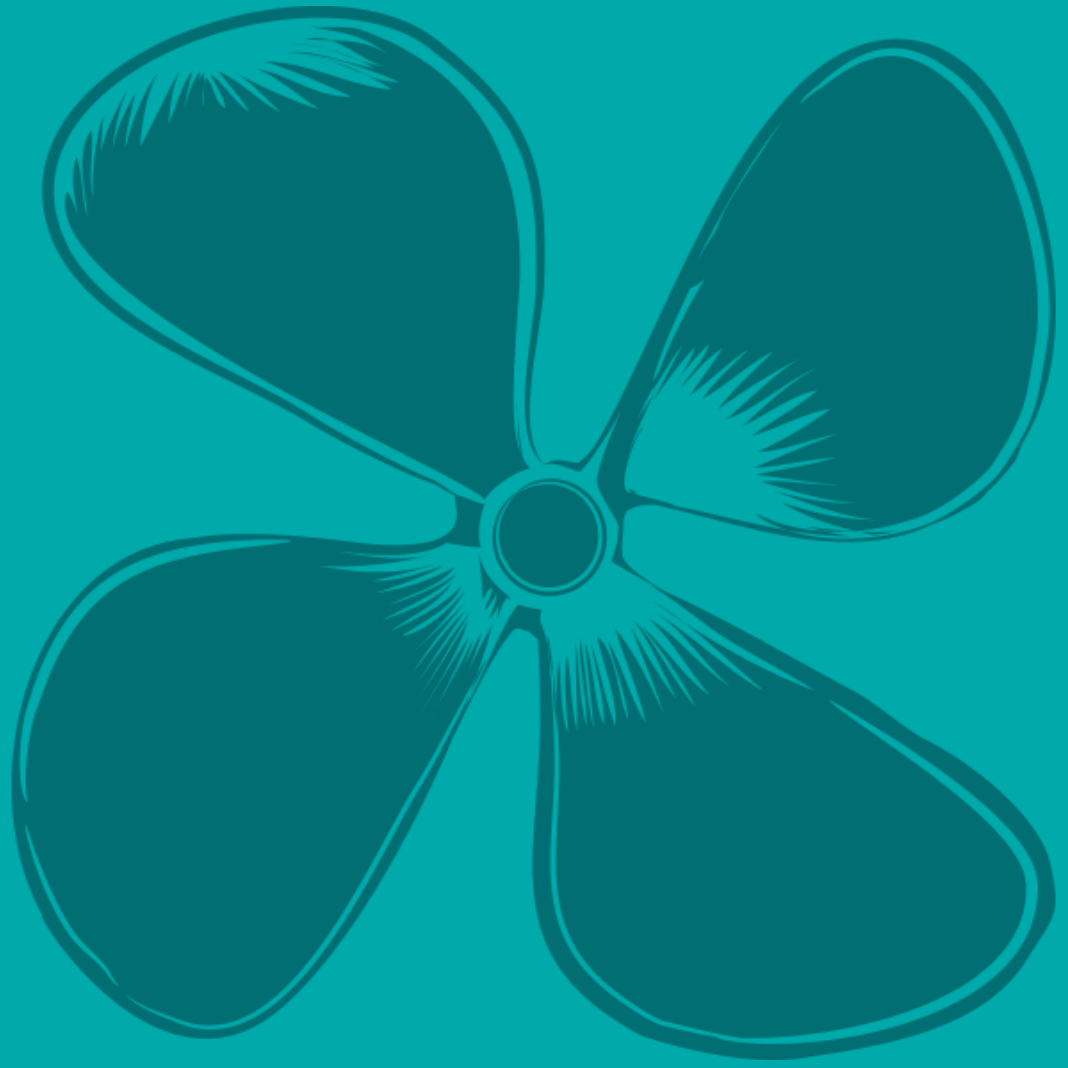
ALEF

Is this something to be worried about?

- Affects all current Outlook versions
- Microsoft decided not to patch it
- Hardly the „next big thing“ in phishing but good to know about

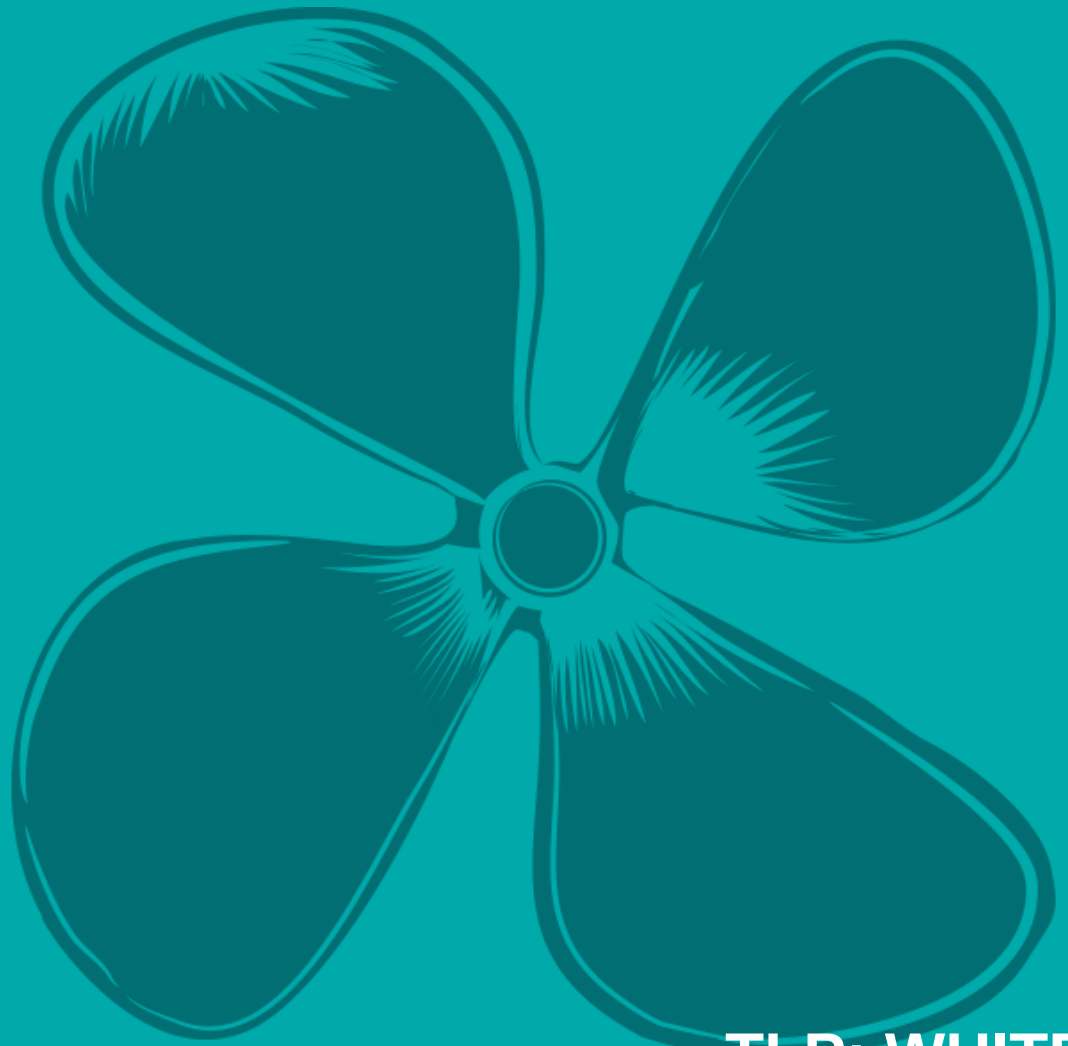
ALEF

Q&A



ALEF

Thank you for your attention



TLP: WHITE