UHH Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

REGIONALES
RECHENZENTRUM

Director

Prof. Dr.-Ing. Stephan Olbrich

25 March 2020

Increased threat from Emotet malware

In recent months, the number of reports of IT security incidents involving the Emotet malware has increased—also at German universities and other public institutions. The Regional Computing Center (RRZ) has implemented effective measures to protect the IT infrastructure. Your mindful use of all information technology and your full attention are required nonetheless.

We urgently ask that you take note of the following information and recommendations for action.

What does Emotet do?

Emotet reads all contact information and emails in the inboxes of infected systems. The hackers then use this information to disseminate the malware further.

What does this mean?

All contacts are sent an email containing seemingly authentic (but fictitious!) content from senders they have been in contact with in the past. As the sender and recipient's names and email addresses are correct in the subject line, opening address, and signature, many people think these messages are genuine. They are tempted to open the malicious attachment or link contained in the message without a second thought.

Once the computer is infected, Emotet downloads further malware, such as the banking trojan Trickbot. These malicious programs cause data leaks or allow criminals to take full control of the system. In several cases known to the Federal Office for Information Security (BSI), this led to major production losses, as entire company networks had to be rebuilt. For you as a user of Universität Hamburg's IT services and also as a private user, an infection can mean data is lost—particularly important access data.

Source:
www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

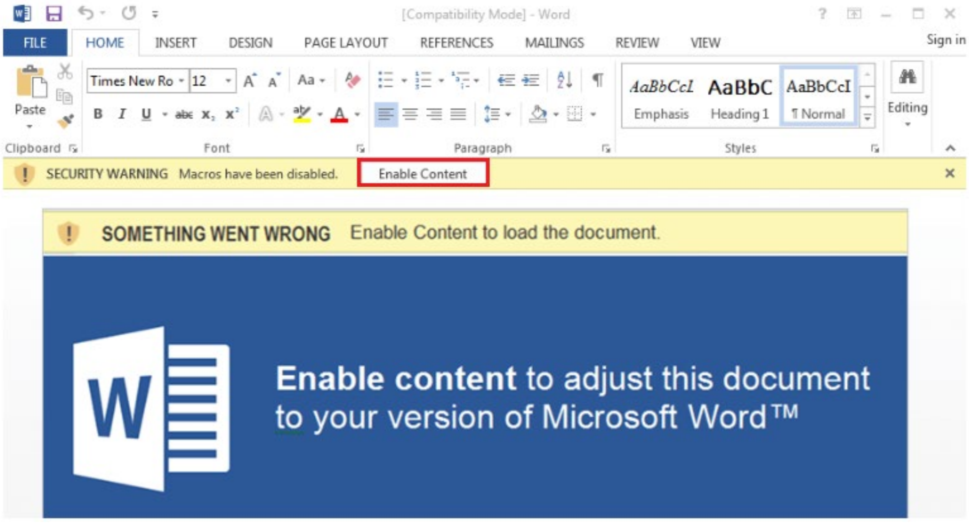
The BSI recommends using the "3-second check" to evaluate incoming messages:

- Do I know the sender's email address (not just the name displayed)?
- Does the subject line make sense?
- Am I expecting an attachment or link?

How can I recognize malicious emails and how can I protect myself?

Never just open attachments or links in emails without a second thought—and heed the following:

- Be aware that your email program does not always display the actual sender's address. Words misspelled in the email text and meaningless sequences of letters and numbers are a telltale sign. If necessary, call the alleged sender to check whether they sent the email.
- Pay particular attention to pages to which links mentioned in the mail direct you. The real link destination is shown in your email program or web browser when you hover the mouse over the link (either directly on the link itself or at the bottom left).
- Do not open documents downloaded from websites you are unfamiliar with.
- If you open email attachments, activate the editing function only when you are 100 percent sure that the attachment and email are genuine. The same applies for saving attachments. It's better to be safe than sorry!
- If you are prompted to "Enable content" in a document (see below), this is a clear warning sign. Never click on the "Enable Content" button!

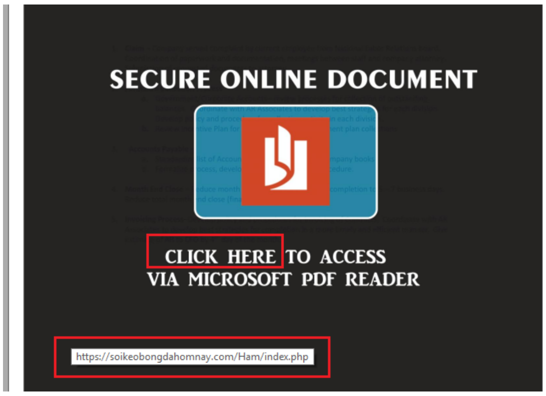


SECURITY WARNING Macros have been disabled. Enable Content

SOMETHING WENT WRONG Enable Content to load the document.

Enable content to adjust this document to your version of Microsoft Word™

- If a document (e.g., a PDF with a reader to view a file—see below) prompts you to follow a link to download software so that you can read a file, do not click on this either.



SECURE ONLINE DOCUMENT

CLICK HERE TO ACCESS VIA MICROSOFT PDF READER

https://soikeobongdahomnay.com/Ham/index.php

What should I do if my computer is infected?

- If, despite all of the precautions taken, your computer is infected (or you suspect that it has been infected), switch your computer off immediately and inform the RRZ without delay. Since the malware may have compromised your email account, it is best to call the RRZ ServiceLine (Tel: +49 40 42838-7790).
- Have your email account and username blocked to prevent any further misuse. Set new passwords for all other services you use the same username for. Remember to never use the same password for different services—especially for private matters.
- Since the malware also transmits personal data, Universität Hamburg's data protection officer must also be informed without delay (datenschutz@uni-hamburg.de). He or she can then decide whether or not to report the incident to the data protection supervisory authority pursuant to the EU General Data Protection Regulation (GDPR).

Be sure to also take note of the latest security warnings on www.rrz.uni-hamburg.de and the general information about IT security on www.rrz.uni-hamburg.de/services/sicherheit.html.