Email-based threats: addressing the human factor

Sebastian Łopieński
CERN Deputy Computer Security Officer
Instead of “why”: a recent data breach at ANU

Public detailed report (Oct. 2\textsuperscript{nd}, 2019)

“The initial means of infection was a sophisticated spear phishing email (targeting a senior staff member)

[..]

Information from victim’s calendar was used to conduct additional spear phishing attacks later in the campaign”

Kudos for being transparent!
E-mail is the main attack vector
E-mail is the main attack vector

It’s very (too) easy and cheap to send e-mails

It’s trivial to fake “From” field

Malicious e-mails contain infected attachments and links to malicious websites
What tactics do adversaries employ?
10.12.2018, 20:37,

Dear Giovanni,
I think this might be fishing!
Can you confirm?
Thanks,

From: Giovanni ✈️✈️✈️ <office.outlook@yandex.com>
Date: 10 December 2018 at 10:42:14 CET

Hi 🤔,

This is safe and secured to access

Get back to me soon as you get this.

Regards
Giovanni ✈️✈️✈️

Scan.pdf
Adobe Acrobat
Secured Document

Adobe Acrobat
PDFXML Document

Click on Download Adobe Document below & verify your email / login to securely access files!

Download Document
Size: 88.7 KB

Adobe Cloud: Have all your files within reach from any device.
Adobe Acrobat
Secured Document

Security Warning

The document is trying to connect to:
https://ruedesnournou.com

Do you trust ruedesnournou.com? If you trust the site, choose Allow. If you do not trust the site, choose Block.

[ ] Remember this action for this site for all PDF documents

Help  Allow  Block  Cancel
1) CONTRACT TERMS AND CONDITION / CERTIFICATE OF COMPLIANCE

2) FUND ALLOCATION / PURCHASE ORDER

3) DELIVERY PERIOD (duration) / PORT OF DESTINATION

4) DELIVERY TERMS / PAYMENT TERMS / QUOTE VALIDITY

someone@example.com

Password

Download
... half a year later ...

Giovanni

Let me know when you are available. There is something I need you to do. I am going into a meeting now with limited phone calls, so just reply my email.

Giovanni

Sent from my iPad
... and another 4 months later

Giovanni <lindajeff99@aol.com>

URGENT
To: <redacted> @cern.ch

I am planning a surprise for some of the staffs with gifts. I need you to get a purchase done, I'm looking forward to surprise some of the staffs with gift cards, I count on you to keep this as a surprise pending when they received it, I need 10 pieces of Amazon $100 face value each gift cards. I need you to get the physical card, then you scratch the card take a picture of the cards pin, attach and email it to me. How soon can you get this done?
I will Reimburse you back later....

Regards
Giovanni
Advanced techniques used by criminals

• **Spear phishing**: malicious mails targeted at specific individuals
  – crafted using information gathered earlier: project names, colleagues names, hierarchy, who is on holidays etc.
  – sent “from” a colleague, a business partner, even the boss
  – “whaling” attacks – targeting top management

• **Using “contacts” lists**: An attacker compromises mailbox of a victim, and sends malicious e-mails “from” the victim to their contacts

• **Joining existing conversation**: An attacker compromises mailbox of a victim, and replies to existing conversations, adding a malicious URL or attachment
How can we defend ourselves and our users?
Technical protection measures (simplified view)

• Traditional **anti-spam filters** (signature-based, blocking certain file types etc.)
• Advanced **anti-malware systems** (behavior-based)
  – “detonating” (opening) attachments in a controlled environment
  – (???) visiting embedded links – very problematic!
• **Hardened end-points computers**, for example:
  – anti-virus software, secure browsers etc.
  – macros disabled in received documents
  – not running as administrator
• **Network protection and detection**
  – e.g. blocking malicious domains at the DNS level
  – only partially effective (computers on the corporate network, no DNS over HTTPS etc.)
Users are our last line of defense
Simulated phishing campaigns at CERN

**Goal**
- raising awareness
  - understanding the scale of the problem

**Approach**
- no spear phishing
- no internal knowledge
- no blaming

**Techniques**
- “malicious” links (2016-2018)
- “malicious” attachment (2019)
Various messages, senders, sender domain etc.

Sonia Abelona <Sonia.Abelona@cern.org>
Sonia Abelona has shared a file with you
To: 

Dear [Name],

Please see the attached for your 2019 contract amendment request.

Regards,
Sonia Abelona
Manager at Human Resources

Federico Campesi <Federico.Campesi@cern.ch>
Federico Campesi has shared a file with you
To: 

Dear [Name],

Please see the attached for report on pension fund balance situation.

Regards,
Federico Campesi
Finance Management

Contract amend...21.doc

Fund balance - confidential.pdf
How many open the Word document?

How many enable macros?

How many follow the link?

Adobe Acrobat Secure Document

How many open the PDF document?

Download 87.3KB

Adobe Cloud: Access your files anywhere, safely

How many follow the link?
If you click on the link, you get redirected to this page:

 Oops... The email and the attachment you have just opened are fake, and potentially malicious!

You just fell for a scam. The attached document that you have opened is fake, and potentially malicious. Your “click” could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify malicious emails and attachments, and what consequences opening them might have for you and your digital assets...
... with hints on **how to identify malicious emails**:

- Is the sender familiar to you?
- Is the e-mail address correct? (for example @cern.ch)
- Does the e-mail address correspond with the sender’s name?
- Is the message correctly phrased, without major typos, in a language that you can understand?

Does the message concern you? Is it related to your work or activities?

Is the message signed (署名)?

Is the message addressed to you?

Do you expect this attachment?

If you have answered any one of those questions with “NO” be vigilant and careful! Delete that message or check with us at [Computer.Security@cern.ch](mailto:Computer.Security@cern.ch) when in doubt.
How many open the Word document? 20%

How many enable macros? 4%

either: 8%

How many follow the link? 5%

How many open the PDF document? 30%?

Download 87.3KB Adobe Cloud: Access your files anywhere, safely

How many follow the link? 14%
What works?

Please see the attached report on pension fund balance situation for your 2019 contract amendment request. with the confidential design report. on your input to our results. on new IT security measures.

From

@cern.com 17%
@cern.org 17%
@cem.ch 18%
@cern.ch 16%
@cern.ch 20%

HEPiX Fall 2015 campaign: Get a voucher for free drinks

Dear sebastian

Dear Sebastian
People respond

• I am unable to contact Ralf Brant (or Brandt!). He is not in the CERN phonebook. Please help. I am trying to send some info.

• I received this mail, as coming from a cern address and headed to me, I trusted it and opened the pdf

• I have received this Email, I am unable to open the attachment and I am starting to worry that it is not from CERN.

• I have opened the attachment, I noticed that the sender address is incorrect (@cerm.ch), I'm confused a bit ... is it an malicious emails!? if yes, what should i do !?

• The email was directed at me with some accurate details.

• The attached file is strange (I could not open it)

• Today morning I was opening my e-mails, as I had much feedback, I've received documentation that I was waiting for. Meanwhile, I got an e-mail improper, but I was not awake enough and I've opened it.

• Since the email address is a CERN address, I thought it's no problem, I downloaded the attachment and tried to open it. However, I cannot open it neither on Linux nor on Windows. I tried to reply to this address but I always get rejected (delivery failure)
A design report of only 35 kB file size sounds suspicious.

I am a summer student who just recently arrived at CERN. Today I received a weird email [...] I opened it. Now I realise how silly that was

as always I detected this mail as the regular test from IT security. I really enjoy them, because they are quite well designed and lead to a very informative site about mail scams and how to detect them.

Could you please explain what is going on? I believe you are violating CERN's code of conduct...
Commercial solutions, open-source tools
Commercial solutions: **simulated phishing campaigns**

- Engagement, gamification
- Classroom courses → **continuous micro-training in work environment**
- Security awareness → **behavior change**

- Examples:
  - every user receives ~3 messages per month (apparently deemed acceptable)
  - growing difficulty of messages, increasing level of "truth", using internal information e.g. names of executives or projects
  - users report malicious mails with a button in Outlook → feeding the SOC

**Is simulated phishing worth the effort?**  Yes
**Should failing phish tests be a fireable offense?**  No
Open-source tools also available

Gophish

SocialFish

Phishing Frenzy

BLACKEYE

FiercePhish
Conclusions
People and technology
... an unsolvable problem?

“I received this mail, as coming from a cern address and headed to me, I trusted it and opened the pdf”