Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
Introduction - whoami

Florian Lukavsky  |  f.lukavsky@sec-consult.com

Security Consultant
Director - SEC Consult Singapore
Passionate about security
Agenda

Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
What is a Fake President Fraud?

= Business E-Mail Compromise or Fake CEO Fraud

**APPROACH**
sophisticated scam, using social engineering techniques
- spear phishing
- vishing

**TARGETS**
businesses
- working with foreign suppliers
- regularly perform wire transfer payments

**GOAL**
unauthorized transfer of funds
Is it common?

+9 months
+13,964 cases
+$ 2.2 billion in losses
from October 2013 through May 2016

22 months
8,179 cases
$800 million in losses
from October 2013 to August 2015

Source: FBI / IC3
Stages of a Fake President Fraud

1. establishing contact
2. creating a pretext (company take-over, urgent purchase, etc.)
3. adversary impersonates CEO, president or senior manager
4. victim is an employee responsible for bank transfers
5. request money transfer
Why do Fake President Frauds work?

- **Authority**: impersonate a CEO
- **Scarcity Urgency**: to stress a pressing matter
- **Obligation**: require the victim to keep the request secret
- **Likability Reciprocity**: the victim was chosen and is trusted by the ‘CEO’
- **Pressure**: shifting the responsibility for success of the ‘deal’ to the victim
Agenda

Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
**Scoular** – US commodities trader
Attacked in June 2014
Lost $17.2 m

Mattel – US toy manufacturing company
Attacked in April 2014
Lost $3 m
Recovered the losses

**Ubiquiti** – US technology company
Attacked in June 2015
Lost $46.7 m
Recovered $9 m

http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/
Crelan – Belgian bank
Attacked in January 2016
Lost €70 m

http://www.standaard.be/cnt/dmf20160119_02077042
**FAAC** – Austrian aviation supplier
Attacked in January 2016
Lost €41.9 m
Stopped another €10.9 m

http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF
LEONI – German manufacturing firm
Attacked in August 2016
Lost €40 m
Agenda

Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
Prevent Fake President Fraud - Organizational

- awareness
- defined processes for payments
- 2-step verification process for unusual payments
- limit public financial or personal information
- strict use of business e-mail address for business purposes
- report to law-enforcement
Prevent Fake President Fraud - Technical

- don’t accept emails with your domain from foreign mail server
- use email signatures / encryption (S/MIME / PGP)
- mark external mails in subject line
- warn before sending to external email addresses
- strong authentication for any web mail (OWA, etc.)
- scan for / register similar domains
Fighting Back – Defrauding the Fraudster

https://blog.kwiatkowski.fr/?q=en/tech-support
Fighting Back – Defrauding the Fraudster

François Wanecq
To: [redacted]
Re: PAYMENT

You are to send:
Bank name:
Account name:
Account number:
Routing number:

And get back.

6 July 2016 at 10:12 PM

12 July 2016 at 8:15 PM

François Wanecq
To: [redacted]
Re: wire instruction.

It was done yesterday. Resending.

12 July 2016 at 8:18 PM

François Wanecq
To: [redacted]
Re: wire instruction.

Happy! :) Thank you.
Email Tracking

Email Tracking Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td><a href="mailto:fakepresident@company.com">fakepresident@company.com</a></td>
</tr>
<tr>
<td>From</td>
<td><a href="mailto:fakepresident@company.com">fakepresident@company.com</a></td>
</tr>
<tr>
<td>Subject</td>
<td>Re: Wire instructions</td>
</tr>
<tr>
<td>Sent on</td>
<td>14-Jul-2016 at 11:47:28 AM (GMT+08:00)</td>
</tr>
<tr>
<td>Opened at</td>
<td>14-Jul-2016 at 12:10:31 PM (GMT+08:00)</td>
</tr>
<tr>
<td>Location</td>
<td>(80% likelihood)</td>
</tr>
<tr>
<td>Recipient IP</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Language</td>
<td>en-us</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Mobile Safari</td>
</tr>
<tr>
<td>Operating System</td>
<td>iOS</td>
</tr>
<tr>
<td>User Agent String</td>
<td>Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F70</td>
</tr>
<tr>
<td>Read Duration</td>
<td>Please see the live tracking details of this email for email read duration.</td>
</tr>
<tr>
<td>Note</td>
<td>In case of Hotmail or Gmail Recipient, Location and IP address related information will not be accurate because Hotmail and Gmail do not disclose the actual IP address of recipient instead, they provide IP address and location of their servers.</td>
</tr>
</tbody>
</table>

Callback Documents

CyberTrap

Email Tracking

Email Tracking Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td><a href="mailto:fakepresident@company.com">fakepresident@company.com</a></td>
</tr>
<tr>
<td>From</td>
<td><a href="mailto:fakepresident@company.com">fakepresident@company.com</a></td>
</tr>
<tr>
<td>Subject</td>
<td>Re: Wire instructions</td>
</tr>
<tr>
<td>Sent on</td>
<td>14-Jul-2016 at 11:47:28 AM (GMT+08:00)</td>
</tr>
<tr>
<td>Opened at</td>
<td>14-Jul-2016 at 12:10:31 PM (GMT+08:00)</td>
</tr>
<tr>
<td>Location</td>
<td>(80% likelihood)</td>
</tr>
<tr>
<td>Recipient IP</td>
<td>[redacted]</td>
</tr>
<tr>
<td>Language</td>
<td>en-us</td>
</tr>
<tr>
<td>Web Browser</td>
<td>Mobile Safari</td>
</tr>
<tr>
<td>Operating System</td>
<td>iOS</td>
</tr>
<tr>
<td>User Agent String</td>
<td>Mozilla/5.0 (iPhone; CPU iPhone OS 8_3 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F70</td>
</tr>
<tr>
<td>Read Duration</td>
<td>Please see the live tracking details of this email for email read duration.</td>
</tr>
<tr>
<td>Note</td>
<td>In case of Hotmail or Gmail Recipient, Location and IP address related information will not be accurate because Hotmail and Gmail do not disclose the actual IP address of recipient instead, they provide IP address and location of their servers.</td>
</tr>
</tbody>
</table>
Agenda

Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
Hey Phil! Did u already take care of the invoice? It’s important!

Frank, which invoice are you talking about?
Ohhh damn!!
It's attached to this mail. Please take care of it.
3 hours later...

What are you talking about?

Frank, I initiated the transfer!
WHAT IF you could identify the fraudster?
Later the same day...

sample image – optical appearance of the combat team may differ
Frank, find attached the confirmation!
Demo
Agenda

Introduction
Background
Prominent cases
Avoid being scammed
Demo
Q&A
SEC Consult in your Region (EMEA)

AUSTRIA
SEC Consult Unternehmensberatung GmbH
Mooslackengasse 17
1190 Vienna
Tel +43 1 890 30 43 0
Email office@sec-consult.com

SWITZERLAND
SEC Consult (Schweiz) AG
Turbinenstrasse 28
8005 Zurich
Tel +41 44 271 777 0
Email office-zurich@sec-consult.com

GERMANY
SEC Consult Deutschland Unternehmensberatung GmbH
Ullsteinstraße 118, Tower B/8th Floor
12109 Berlin
Tel +49 30 30807283
Email office-berlin@sec-consult.com

LUXEMBOURG
SEC Consult Luxembourg S.àr.l.
25 avenue de la Gare
4131 Esch-sur-Alzette
Email office-luxembourg@sec-consult.com

RUSSIA
CJCS Security Monitor
5th Donskoy proyezd, 15, Bldg. 6
119334, Moscow
Tel +7 495 662 1414
Email info@securitymonitor.ru

LITHUANIA
UAB Critical Security, a SEC Consult company
Sauletekio al. 15-311
10224 Vilnius
Tel +370 5 2195535
Email office-vilnius@sec-consult.com