

Cybersecurity at CERN and in general

Sebastian Łopieński

CERN Computer Security Team

Polish Teacher Programme

February 2021

Why?

I am protected... ?



I am protected.... ?



**No, not
really**

An incident in September 2008



The Telegraph.co.uk website header features the logo and a "BEST CONSUMER ONLINE PUBLISHER" award badge from AOL UK. The navigation menu includes links for Home, News, Sport, Business, Travel, Jobs, Motoring, and Telegraph TV. A sidebar on the left lists "Earth home", "Earth news", "Earth watch", "Comment", "Charles Clover", and "Greener living". The main article snippet is titled "Hackers infiltrate Large Hadron Collider systems and mock IT security" by Roger Highfield, Science Editor, and is dated "Last Updated: 4:01pm BST 12/09/2008".

The Times Online website header includes the "News Site of the Year" award from "The 2008 Newspaper Awards". The navigation menu lists "NEWS", "COMMENT", "BUSINESS", "MONEY", "SPORT", "LIFE & STYLE", "TRAVEL", and "DRIVING". A secondary menu lists "UK NEWS", "WORLD NEWS", "POLITICS", "ENVIRONMENT", "WEATHER", "TECH & WEB", and "TIMES ONLINE". The article snippet is titled "Hackers break into CERN computer – to show up its 'schoolkid' security" and is dated "September 13, 2008".

..etc...etc...

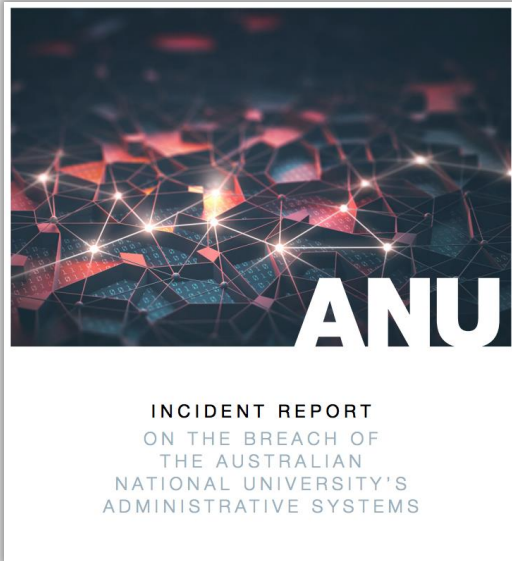
A major data breach at Australian National University

Public detailed [report](#) (Oct. 2nd, 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”*



People and technology



Which links goes to *eBay*?

<http://secure-ebay.com>

<http://www.ebay.com/cgi-bin/login?ds=1%204324@124.136.10.203/p?ufgs...>

<http://www.ebay.com/ws/eBayISAPI.dll?SignIn>

http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default

Technology is often complex

<http://secure-ebay.com>

<http://secure.ebay.com>

<http://www.ebay.com/cgi-bin/login?ds=1%204324@124.136.10.203/p?ufgs...>

<http://www.ebay.com/ws/eBayISAPI.dll?SignIn>

The logo for ebay.com, featuring the word "ebay" in a bold, lowercase, sans-serif font, followed by ".com" in a smaller, lowercase, sans-serif font. The logo is enclosed in a thin black rectangular border.

http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default

What issues do we deal with at CERN?



C3 ~ RET

@c3retc3

Follow

#CERN discloses passwords, source code and tickets to Web spiders

6:03 a.m. - 29 Sep 2015



Dan Tentler

@Viss

Follow

someone asked earlier if I was gonna find CERN - here's one (I got their CERT guys email. I'll notify) pic.twitter.com/zu180KzyBo

Reply Retweet Favourite More

```

Welcome to CERN Virtual Machine, version 2.6.0
unZ209280-01 login: --- a new cntuser directory has been created in your HOME directory
-----
----- LHCb Login u7r10p4 -----
*      Building with gcc46 on slc5 x86_64 system (x86_64-slc5-gcc46-opt)      *
-----
--- User release_area is set to /opt/dirac/cntuser
--- LHCbPROJECTPATH is set to:
/cunfs/lhcb.cern.ch/lib/lhcb
/cunfs/lhcb.cern.ch/lib/lcg/releases
/cunfs/lhcb.cern.ch/lib/lcg/app/releases
/cunfs/lhcb.cern.ch/lib/lcg/external

```

RETWEETS

7

FAVOURITES

12



11:59 am - 14 Aug 2014

Flag media

<sc0rp> nice

<MLT> using the exploit on **CERN** would be win, hacking the people who created the internet :P

<sc0rp> haha

News

- ▶ [Special Ops Armed with Rapid DNA Scanners: "Get Ready for Advanced Biometric Warfare"](#)
- ▶ [California Moves to Force Childcare Workers to Vaccinate or Be Criminals](#)
- ▶ [West Virginia Bill to Keep Guard Troops Out of Unconstitutional Foreign Wars Killed by Pentagon Threats](#)
- ▶ [EXCLUSIVE: LEAKED REPORT PROFILES MILITARY, POLICE MEMBERS OF OUTLAW MOTORCYCLE GANGS](#)
- ▶ [A key source clues me in on TPP code of silence](#)
- ▶ [It Is Mathematically Impossible To Pay Off All Of Our Debt](#)
- ▶ ["Raider Focus" - Colorado Braces For Largest War Games](#)



[Back to Forum](#)



[Post New Thread](#)



[Reply](#)



[View Favorites](#)

[Join Now, Free! \(& No Ads!\)](#) [Forgot Your Password?](#)

Email

Password

Rate this Thread

Absolute BS Crap Reasonable Nice Amazing

[Bottom](#) [Search Replies](#) [Previous Page](#) [Next Page](#)

Do you think it's possible for the CERN LHC to be hacked?

Anonymous Coward
User ID: 9578086
 United States
05/25/2015 10:42 PM
[Report Abusive Post](#)
[Report Copyright Violation](#)

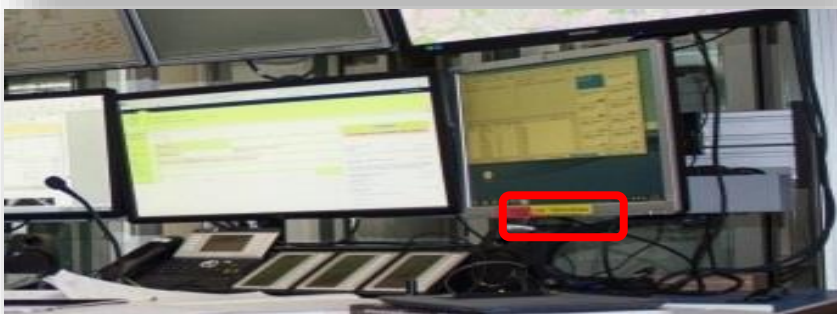
Do you think it's possible for the CERN LHC to be hacked?

Shouldn't it have the same level of protections as a nuclear power plant? Yet I feel it probably does not...

Anonymous Coward
User ID: 69274093
 United States
05/25/2015 11:18 PM
[Report Abusive Post](#)
[Report Copyright Violation](#)

Re: Do you think it's possible for the CERN LHC to be hacked?

Scary thought. Hollywood hit..
Really cern has been hacked, it is ran by mad scientists, hell bent on crazy.
These are the type of people that jump from rocks with wing suits with life mentality.
They want crazy. Cern is a weapon, the biggest and most psychotic ever created.



CERN Bulletin

News Articles Official News Training Announcements Events
Staff Association

english | français

search

Issue No. 20-21/2014 - Monday 12 May 2014

No printable version available - Subscribe:

Polarisation confirmed

Celebrating with our neighbours

LS: Report: PS Booster prepares for beam

From the drawing board to the test bench

Data defenders

The "Karma Level Sevvy Bottom" awards are back at CERN

Winter Atomiades 2014: CERN skiers win 31 medals!

BEHIND THE SCENES OF GS: NOTHING LEFT TO CHANCE

The AS (Alarm Systems) Section in the GS-ASE Group is, as its name suggests, in charge of the various alarm systems spread across CERN's many sites. Its mission? To install, manage and maintain more than 26,000 alarms of all types located both above ground and in the tunnels.



Detection

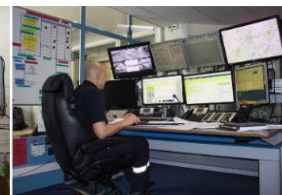
Among these systems, the best known are of course the heat and/or smoke detectors, which quickly raise the alarm in the event of a fire. CERN has 8500 of

these devices in total. In combination with these, evacuation alarms are also found all over the which is then connected to a transmission unit. From here, the information – for example, which type of alarm has been activated in which building – is transmitted to the Fire Brigade's Safety Control Room (SCR) and to the CERN Control Centre (CCC). "The information is transferred via two channels," explains Henrik Nissen. "The first channel is a basic electrical (wire) network which, by its very nature, ensures a very high level of reliability. The second channel is a computer network which, although it allows more precise information to be transferred, is not as reliable as the first." All of the alarms essential for the safety of people and equipment (level 3 alarms), as well as vital technical alarms (for cryogenics, for example) always use both channels. This redundancy ensures that the information is transmitted whatever happens.

On the maintenance side, each of the 11,000 level 3 alarms is tested every year. This is a mammoth task which requires the expertise of seven people working full time in close cooperation with CERN's Fire Brigade.

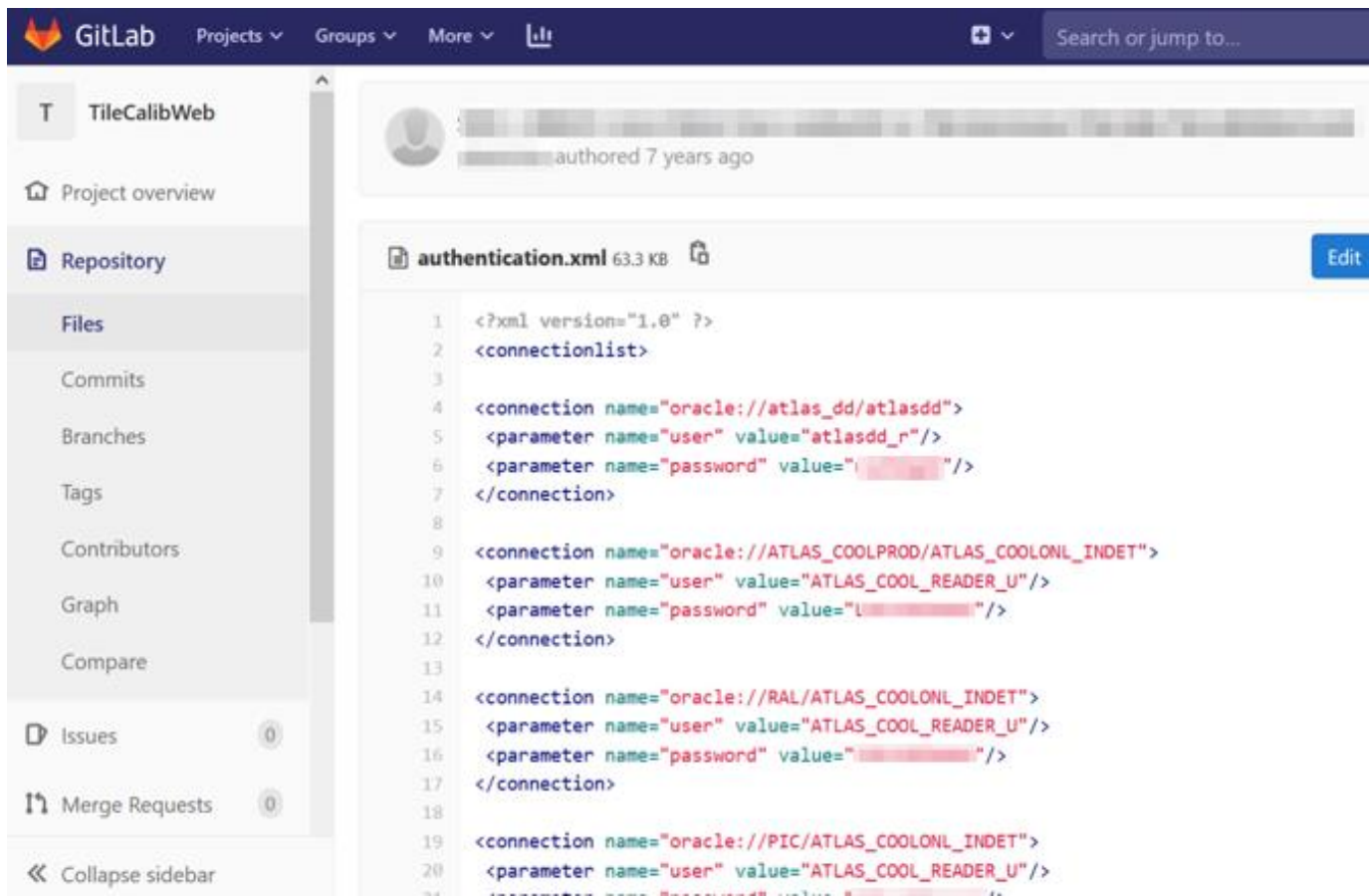


Test platform for detecting gas (including ODH). The bottles at the bottom of the image contain different types of gas used for tests.



The Fire Brigade's Safety Control Room, which receives level 3 alarms.

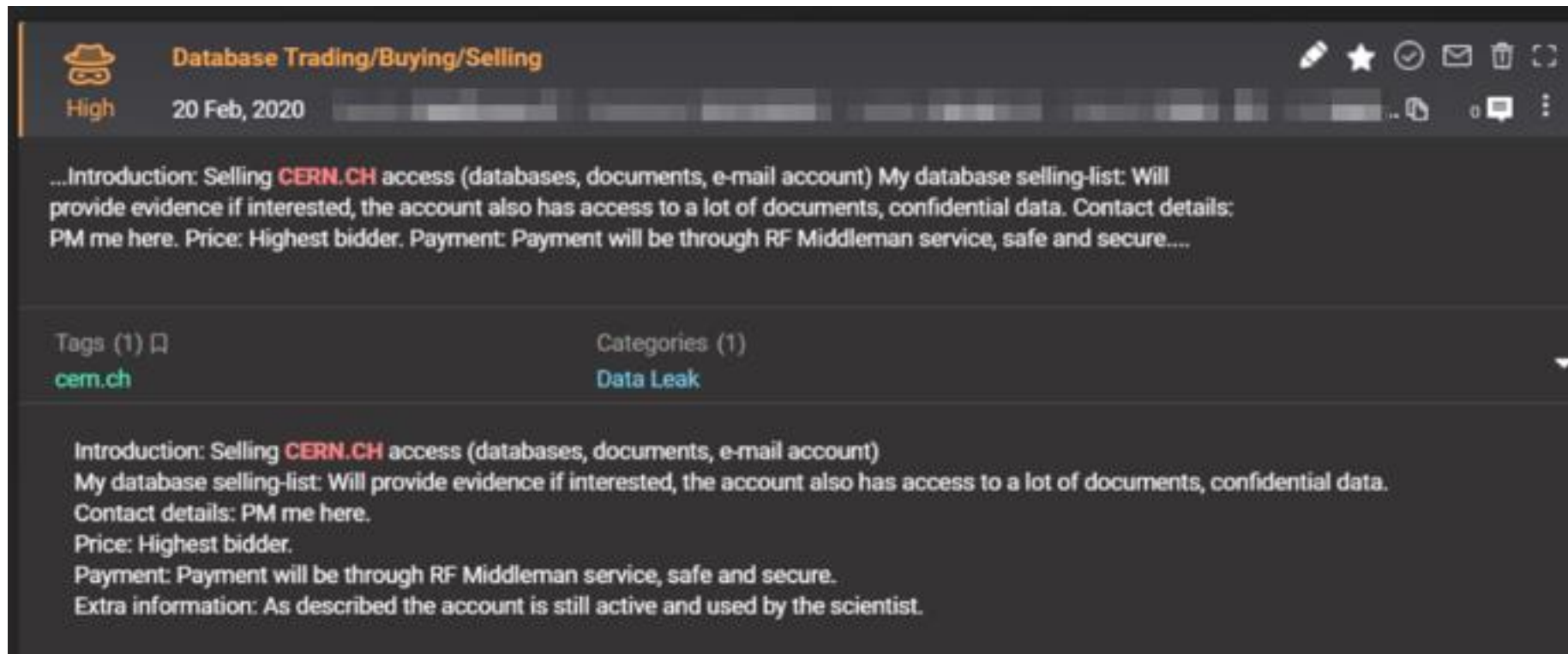
Exposed passwords



The screenshot shows the GitLab interface for a repository named 'TileCalibWeb'. The file 'authentication.xml' (63.3 KB) is displayed, containing XML configuration for database connections. Several connections are listed, each with a 'password' parameter that has been redacted with a pink box, indicating that the passwords are exposed in the source code.

```
1 <?xml version="1.0" ?>
2 <connectionlist>
3
4 <connection name="oracle://atlas_dd/atlasdd">
5   <parameter name="user" value="atlasdd_r"/>
6   <parameter name="password" value="XXXXXXXXXX"/>
7 </connection>
8
9 <connection name="oracle://ATLAS_COOLPROD/ATLAS_COOLONL_INDET">
10  <parameter name="user" value="ATLAS_COOL_READER_U"/>
11  <parameter name="password" value="XXXXXXXXXX"/>
12 </connection>
13
14 <connection name="oracle://RAL/ATLAS_COOLONL_INDET">
15  <parameter name="user" value="ATLAS_COOL_READER_U"/>
16  <parameter name="password" value="XXXXXXXXXX"/>
17 </connection>
18
19 <connection name="oracle://PIC/ATLAS_COOLONL_INDET">
20  <parameter name="user" value="ATLAS_COOL_READER_U"/>
21  <parameter name="password" value="XXXXXXXXXX"/>
```

CERN data stolen and sold on the Dark Web



The image shows a screenshot of a dark web marketplace interface. At the top, there is a navigation bar with a hat icon, the text "Database Trading/Buying/Selling", and a date "20 Feb, 2020". To the right of the navigation bar are several utility icons: a pencil, a star, a checkmark, an envelope, a trash can, and a refresh icon. Below the navigation bar, the main content area displays a listing for "CERN.CH" access. The listing text includes: "...Introduction: Selling CERN.CH access (databases, documents, e-mail account) My database selling-list: Will provide evidence if interested, the account also has access to a lot of documents, confidential data. Contact details: PM me here. Price: Highest bidder. Payment: Payment will be through RF Middleman service, safe and secure....". Below the listing text, there are two sections: "Tags (1)" with the tag "cern.ch" and "Categories (1)" with the category "Data Leak". At the bottom, there is a detailed introduction for the listing: "Introduction: Selling CERN.CH access (databases, documents, e-mail account) My database selling-list: Will provide evidence if interested, the account also has access to a lot of documents, confidential data. Contact details: PM me here. Price: Highest bidder. Payment: Payment will be through RF Middleman service, safe and secure. Extra information: As described the account is still active and used by the scientist."

Database Trading/Buying/Selling

High 20 Feb, 2020

...Introduction: Selling **CERN.CH** access (databases, documents, e-mail account) My database selling-list: Will provide evidence if interested, the account also has access to a lot of documents, confidential data. Contact details: PM me here. Price: Highest bidder. Payment: Payment will be through RF Middleman service, safe and secure....

Tags (1) [cern.ch](#)

Categories (1) [Data Leak](#)

Introduction: Selling **CERN.CH** access (databases, documents, e-mail account)
My database selling-list: Will provide evidence if interested, the account also has access to a lot of documents, confidential data.
Contact details: PM me here.
Price: Highest bidder.
Payment: Payment will be through RF Middleman service, safe and secure.
Extra information: As described the account is still active and used by the scientist.

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07-\$100
2	2	Bank account credentials	16%	19%	\$10-\$900
3	3	Email accounts	10%	7%	\$1-\$18
4	13	Attack tools	7%	2%	\$5-\$650
5	4	Email addresses	5%	7%	\$1/MB-\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50-\$120
7	6	Full identities	5%	5%	\$0.50-\$20
8	14	Scam hosting	4%	2%	\$10-\$150
9	5	Shell scripts	4%	6%	\$2-\$7
10	9	Cash-out services	3%	4%	\$200-\$500 or 50%-70% of total value

Item	Bulk Prices Observed	Unit Price
Credit card information	10 credit cards for \$17	\$1.70
	100 credit cards for \$100	\$1.00
	1000 credit cards for \$300	\$0.30
	750 credit cards for \$50	\$0.07
Credit card dumps	101 dumps for \$50	\$0.50
Full identities	30 full identities for \$20	\$0.67
	100 full identities for \$50	\$0.50

Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select	
372845	AMEX	Charles S	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
528713	MasterCard	Christopher B	US	Chicago, IL		Y	N	Y	40\$	<input type="checkbox"/>
645450	DISCOVER	C MC Kelly	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
371527	AMEX	C Steven	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
646880	DISCOVER	Chris Leung	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
651920	DISCOVER	Chris J	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
645857	DISCOVER	C Brandon	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
371198	AMEX	C Christopher	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
534246	MasterCard	Chris M	US	Los Angeles		Y	Y	Y	40\$	<input type="checkbox"/>
371726	AMEX	Chris S	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
537161	MasterCard	Chris A	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>
447639	VISA	Chris S	US	Los Angeles		Y	N	Y	40\$	<input type="checkbox"/>

PLASTIQUE SHOP

[MAIN](#) | [CHECKER](#) | [BALANCE CHECKER](#) | [Support](#) | \$0.00 | [my cards](#) | [logout](#)

Sort

NAME	TYPE	NUMBER	CV2	EXP	Co.	Addr1	City	State	ZIP	Country	\$		
Vernon *****	Visa	443460*****	***	11/2013		** Charles Street	Kew	VIC	Victoria	****	Australia	6\$	+0.4\$ show check
wille *****	VISA	413821*****	***	09/2012		**** old columbia pike #****	silver spring	MD		****	United States	2\$	+0.4\$ show check
Tony ****	AMEX	377232*****	****	10/2015		**** Rock Meadow Cir	High Point	NC		****	United States	6\$	+0.4\$ show check
Beth *****	VISA	479370*****	***	02/2015		*** N East St	Carlisle	PA		****	United States	3\$	+0.4\$ show check
LB *****	Visa	423954*****	***	10/2013		** Fairlie Street	Mount Gambler	SA	South Australia	****	Australia	6\$	+0.4\$ show check

http://securityresponse.symantec.com/en/ca/threatreport/topic.jsp?id=fraud_activit_y_trends&aid=underground_economy_servers

Cybercriminals against you and me

How cyber-criminals make money?



e-banking trojans



phishing online accounts



identity theft



ransomware



extortion and other scams



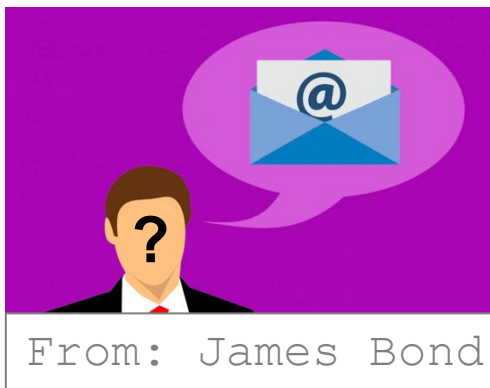
cryptocurrency mining¹⁸

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



Let's see some of criminals' tactics

Example 1

How to trick a victim
(without even infecting their computer)

Example 2

How to steal victim's password
and take over their online account

Standard phishing

● Mail Delivery System <[redacted]@cern.ch>

24 July 2019 at 08:36

MS

Message Delivery Status Notification (Failure)

To: [redacted]@cern.ch

Hello [redacted]
[redacted]@cern.ch

Your messages are now returning a failure delivery because your email has not been verified, you are required to confirm your email account to restore normal email delivery.

This helps us stop automated programs from sending you spam.

[Confirm \[redacted\]@cern.ch](#)

Please note
• Logi
man
Once Verifie
Sincerely,
cern mail delivery system

https://
microsoftof7ahw99n6twblh.z13.web.core.window
s.net/index.php?
c=eee010ae0e015ae0e014ae05ae0.e08ae0e01
6ae019a-
e4e011ae014ae02ae0e08ae1eeee01ae1e013ae0
10a.e01ae05a

so in a
2 Hours

Malicious link

Legitimate links

This is a mandatory service communication for [redacted]@cern.ch.
This message was sent from an unmonitored e-mail address. Please do not reply to this message.
[Privacy](#) | [Legal](#)

http://click.email.microsoftonline.com/?
qs=d306d1daab078722535d35b5ecac1aba5f08
f80731a1b3192b6b6d6198c35cc9d4370eaec2b
d374e44641c036f61e2c5

Example 3

How to infect victim's computer,
and steal their passwords

From: Giovanni [REDACTED] <office.outlook@[REDACTED]>
Date: Monday, 10 December 2018 at 10:
To: [REDACTED]
Cc: [REDACTED]

10.12.2018, 20:37, [REDACTED]

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

Subject: Giovanni [REDACTED] has shared a

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

Hi [REDACTED],

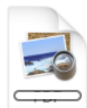
This is safe and secured to access

Get back to me soon as you get this .

Regards
Giovanni [REDACTED]

Please see the attached for your action

Regards
Giovanni [REDACTED]



Scan.pdf


Scan (1).pdf - Adobe Reader

File Edit View Window Help

Open | [Icons] | 1 / 1 | 105% | [Icons] | Tools | Fill & Sign | Comment


Sign In

▼ Export PDF

Adobe ExportPDF 

Convert PDF files to Word or Excel online.

Select PDF File:

 Scan (1).pdf 1 file / 51 KB

Convert To:

Microsoft Word (*.docx) ▼

Recognize Text in English(U.S.)
[Change](#)

► Create PDF


► Edit PDF

► Combine PDF

► Send Files

► Store Files

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://ruedesnounou.com>

Do you trust ruedesnounou.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](#)

Sign In

Export PDF

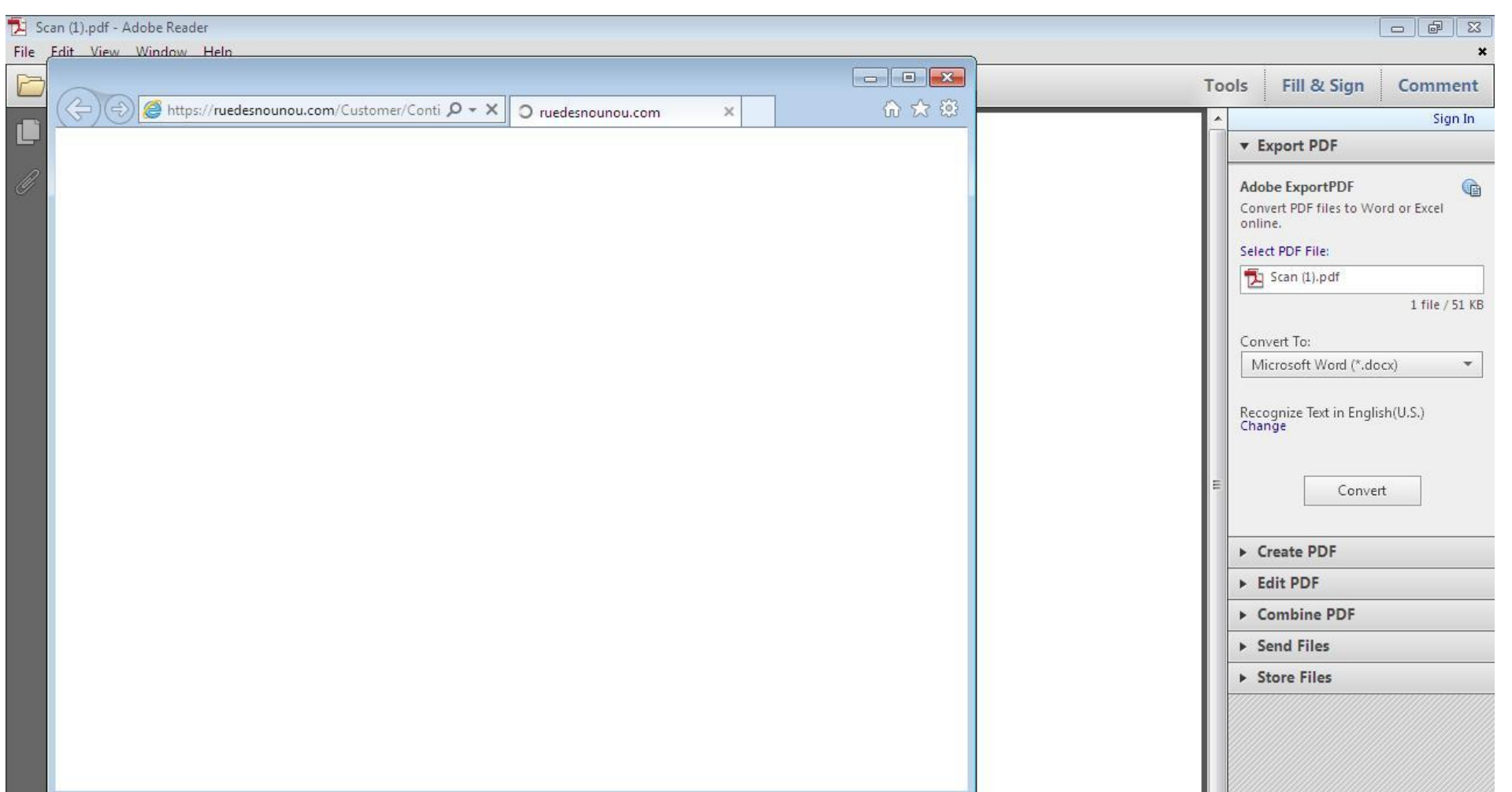
Adobe ExportPDF
Convert PDF files to Word or Excel online.

Select PDF File:
Scan (1).pdf
1 file / 51 KB

Convert To:
Microsoft Word (*.docx)

Recognize Text in English(U.S.)
Change

► Create PDF
► Edit PDF
► Combine PDF
► Send Files
► Store Files



F

FILE HOME INSERT DATA REVIEW VIEW Tell me what you want to do OPEN IN EXCEL

Clipboard: Undo, Paste, Cut, Copy

Font: Calibri, 11, Bold, Italic, Underline, Text Color, Background Color, Font Color

Alignment: Wrap Text, Merge & Center

Number: ABC 123, Number Format

Tables: Survey, Format as Table

Cells: Insert, Delete

Editing: AutoSum, Clear, Sort, Find

fx

	A	B	C	D	E	F	N	O	P	Q	R	S	T	U
1		PAGE 1/40												
2														
3														
4														
5														
6														
7														
8														
9														
10														
11														
12														
13														
14														
15														
16														
17														
18														
19														

Office Excel

someone@example.com

Password

Download

Starting...

CONFIDENTIAL DOCUMENT

... half a year later ...

● Giovanni [redacted] <angelavidos340@gmail.com>

19 June 2019 at 12:33

Respond

To: [redacted]@cern.ch>

[redacted],

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 [redacted] <lindajeff99@aol.com>

Junk - CERN Yesterday at 17:13

URGENT

To: [redacted] <[redacted]@cern.ch>

[redacted]
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 [redacted]

Bonus

Advanced techniques

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 colleagues, a business partner, even the boss
- **Using “contacts” lists**: An attacker compromises mailbox of a victim, and send 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 attachment

So how can I defend myself?

Defense – golden rules

Rule 1: do not trust email

- *From field can be faked* - **anyone** can send an mail as president@whitehouse.gov
- *Don't follow links* from suspicious e-mails
 - if in doubt, just type the URL in the browser
- *Don't open unexpected attachments*, don't enable macros

Rule 2: do not fall for scams and phishing attacks

- No, you haven't won or inherited a fortune, or been offered a great deal
- No, your bank / PayPal / webmail doesn't ask you to "confirm" your account
- No, your CEO/boss doesn't secretly ask you to make a "special" payment/transfer
- No, technical support doesn't call or e-mail you to help you

Defense – golden rules

Rule 3: be careful when browsing the web

- Think before you click
- Make sure you *really* are on the correct website
- Don't install any untrusted software downloaded from the web

Rule 4: protect your computer

- Keep your operating system (Windows, Mac OS etc.) updated
- Keep your software updated (especially the browser and its plugins/extensions)
- Use an anti-virus, keep it updated

Rule 5: protect your passwords and online accounts

- Use strong passwords, and use password managers
- Don't reuse password (same password on different websites)
- Enable strong authentication (multi-factor) whenever possible

What about social media?
Privacy and security risks

“On the Internet, nobody knows you’re a dog”



By The New Yorker, Fair use,
<https://en.wikipedia.org/w/index.php?curid=13627120>

Do not trust blindly
people that you only met online

We all use these services...



Snapchat

Instagram



WhatsApp

Social media + cloud services: basic rules

- What you post/share privately may become public
- Once posted/shared, it will stay forever, even if you “delete”
- **Think before you upload, post, share or comment online:**
 - *Am I giving up my privacy?*
 - *Could I be ashamed of it later?*
 - *Would I like my parents or employer to see it?*
- **Do not take inappropriate or intimate pictures and videos**

We all use these services... **but who pays for them?**



Instagram



Snapchat



WhatsApp

We all use these services... **but who pays for them?**

TikTok



facebook

**If you are not paying,
then **you** are the product**

Snapchat

YouTube

WhatsApp

Data is knowledge, data is power

After some time, these services know you better than your family, better than your friends, sometimes even better than you know yourself

your plans

your interests

your worries

how you look like

where you have been,
and with whom

what you have been doing

your health

Conclusions

Final words

- Be aware of the risks, so that you don't become a victim
- Protect
 - **your accounts** (social accounts, Google/Apple, email etc.)
 - **your computer, smartphone, tablet**
 - **your data** (pictures, documents)
 - **your privacy** (who you are)
- **Think before you click**

