

Computer Security in 2019:

Where we are? What to expect?

How to defend our organizations?

Sebastian Łopieński

CERN Deputy Computer Security Officer

*(with input from S.Lueders, R.Wartel, L.Valsan,
V.Brillault, E.Cruz and other colleagues)*

4 July 2019

CERN openlab summer student lectures

People and technology



2014: Vulnerabilities in cryptography



Heartbleed

(remote information disclosure in OpenSSL)

GnuTLS

(flawed X.509 certificate verification checks)

Microsoft SChannel

(remote code execution vulnerability)

POODLE

(MITM attack exploiting a fallback to SSL 3.0 to decrypt traffic)

FREAK

(MITM attack downgrading SSL to weak “export-grade” encryption)

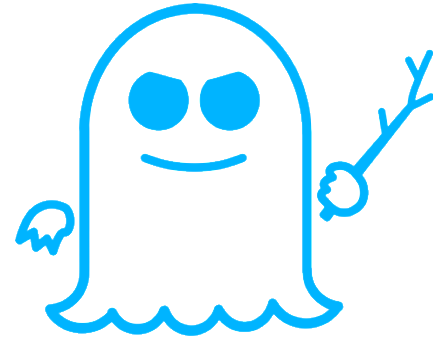
What will 2018 be remembered for?

Waking up to 2018: Intel hardware vulnerabilities



MELTDOWN

```
meltdown:  
mov al, byte [rcx]  
shl rax, 0xc  
jz meltdown  
mov rbx, qword [rbx + rax]
```



SPECTRE

```
if (x < array1_size)  
    y = array2[array1[x] * 256];
```

... it became a tradition

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

Q2 2018 SPECULATIVE EXECUTION SIDE CHANNEL UPDATE

Q3 2018 SPECULATIVE EXECUTION SIDE CHANNEL UPDATE

INTEL® SERVER BOARDS FIRMWARE ADVISORY

... it became a tradition

THE LATEST SECURITY INFORMATION ON INTEL® PRODUCTS.

Q2 2018 SPECULATIVE EXECUTION SIDE CHANNEL UPDATE

“Variant 3a”: Rogue System Register Read (CVE-2018-3640)

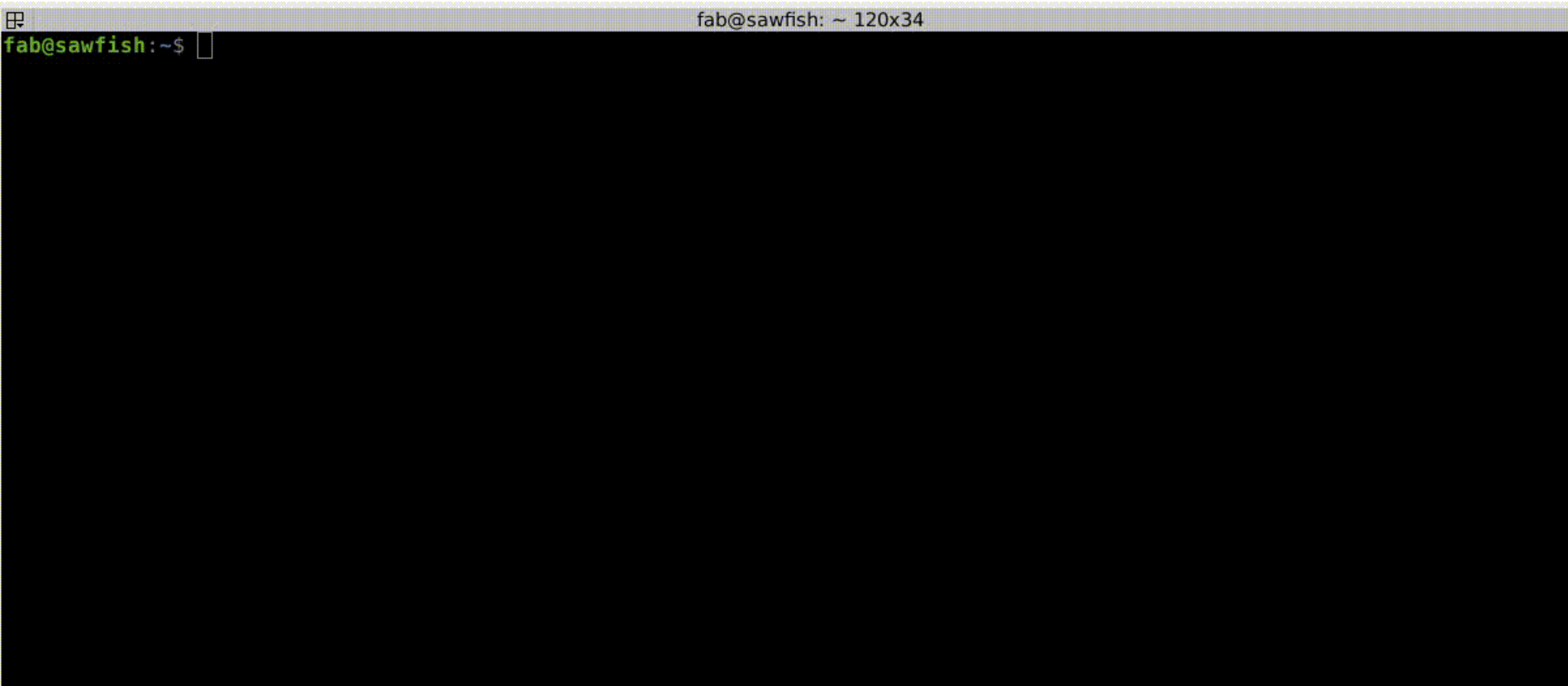
- unauthorized disclosure of data from system registers
- **no software mitigation, purely a hardware issue, requires microcode update**

“Variant 4”: Speculative Store Bypass (CVE-2018-3639)

- similar to “Spectre v1”, except that it leverages Speculative Store Bypass
- an unprivileged user could read privileged system memory, or memory outside of a sandboxed environment (web browser, JIT execution)
- **requires microcode fix + updates to the Linux kernel and virtualization components**
- affects CPUs of various microarchitectures from: Intel, AMD, ARM, IBM...

Critical vulnerabilities in HP iLO: authentication bypass, local and remote code execution

Critical vulnerabilities in HP iLO: authentication bypass, local and remote code execution



From Airbus security lab: https://github.com/airbus-seclab/ilo4_toolbox

OK, so hardware can be vulnerable

What if hardware is *made* vulnerable?

**Bloomberg
Businessweek**

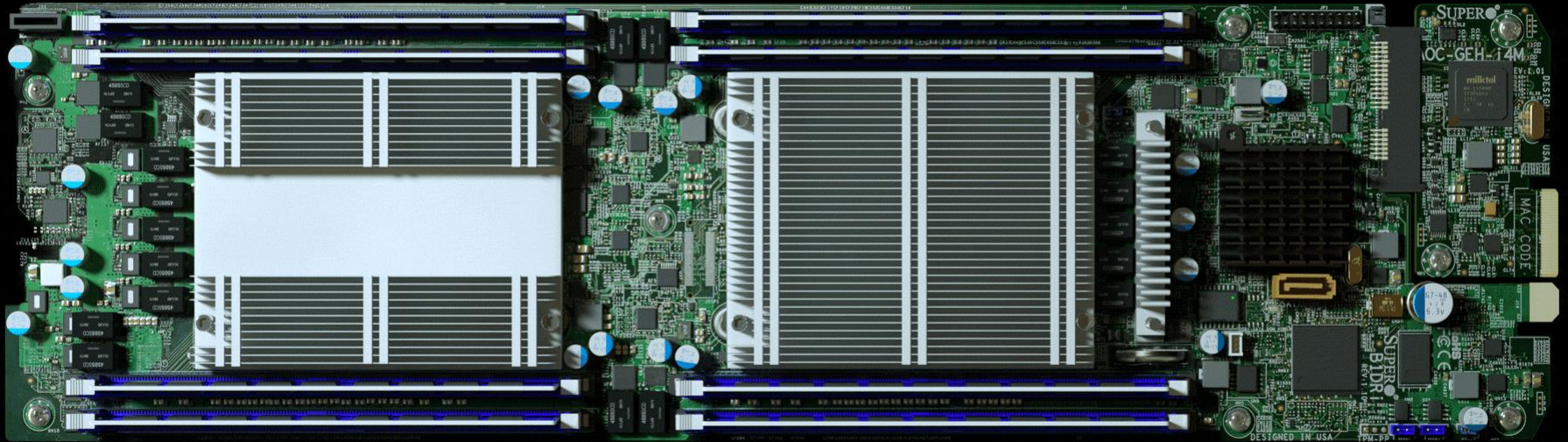
October 8, 2018

The Big Hack

How China used
a tiny chip to
infiltrate America's
top companies

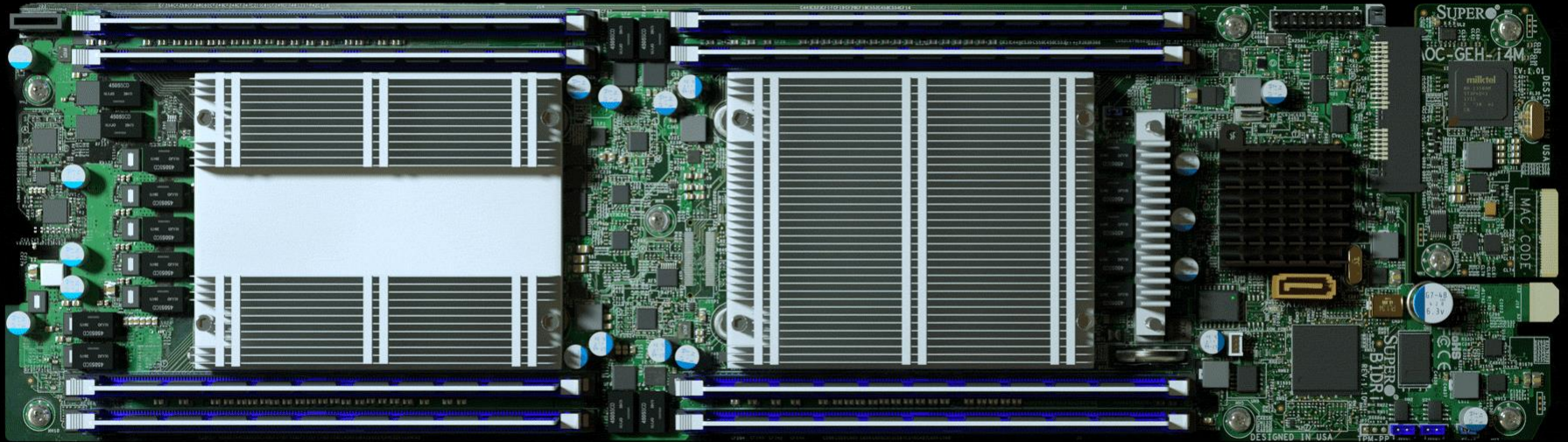


Supply chain attacks



From <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

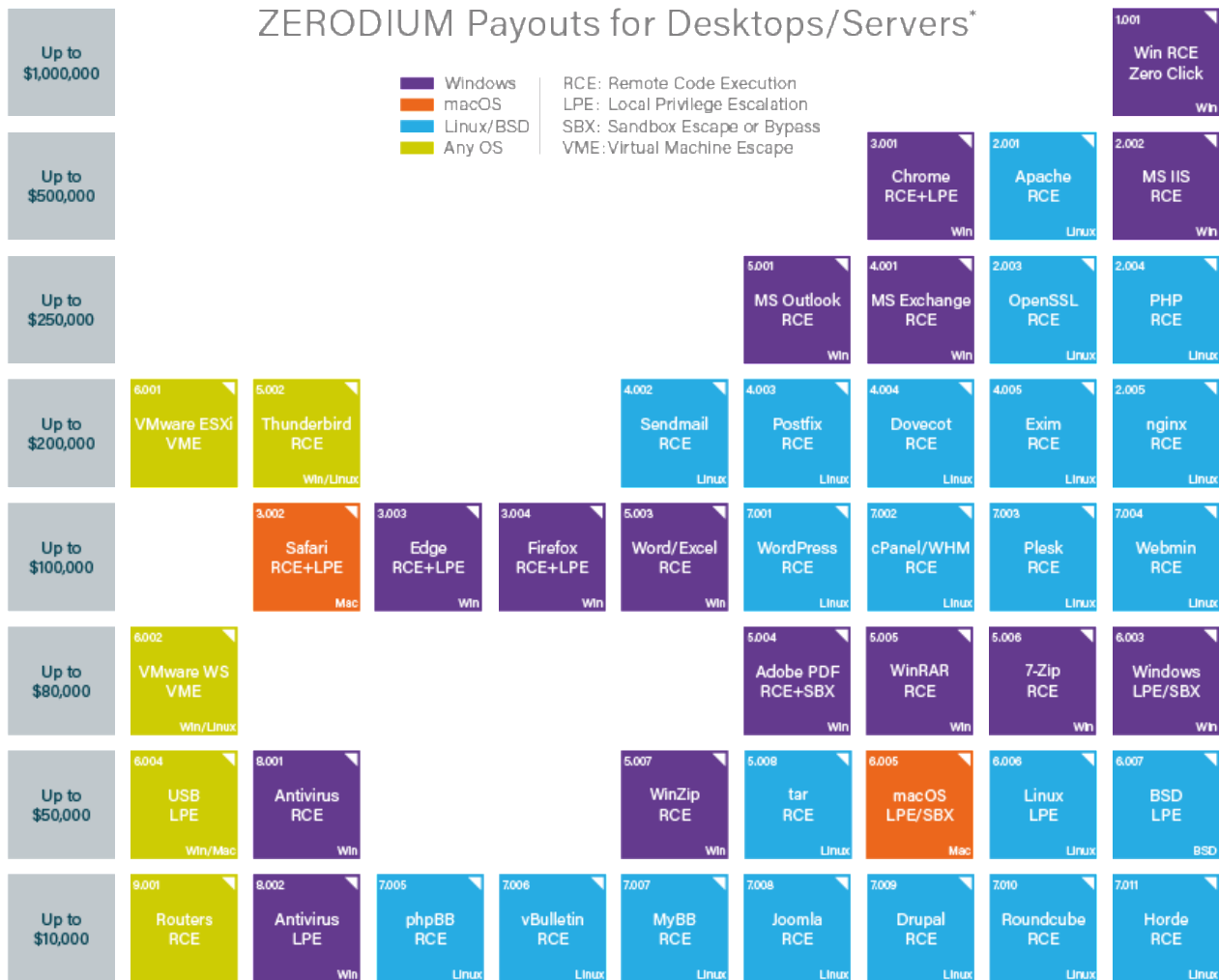
Supply chain attacks



From <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

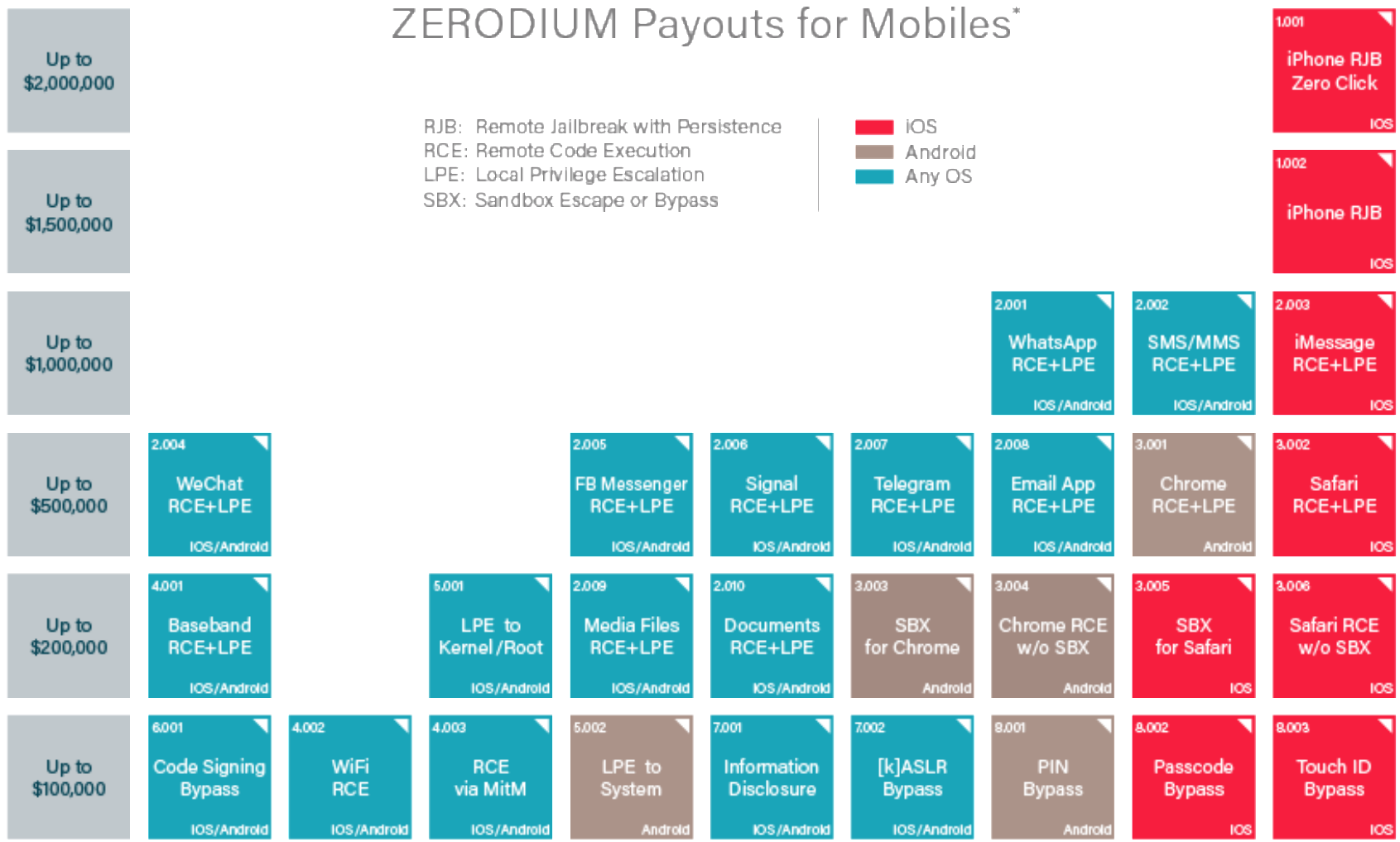
Resourceful adversaries

ZERODIUM Payouts for Desktops/Servers*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

ZERODIUM Payouts for Mobiles*



RJB: Remote Jailbreak with Persistence
 RCE: Remote Code Execution
 LPE: Local Privilege Escalation
 SBX: Sandbox Escape or Bypass

■ iOS
■ Android
■ Any OS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

CVE-2018-8589: zero-day vulnerability in Edge browser

```
mov     eax, [ebp+var_38.Right]
sub     eax, ecx
mov     [ebp+var_14], eax
mov     eax, [ebp+var_38.bottom]
mov     [ebp+var_6C], ecx
mov     ecx, [ebp+var_38.top]
sub     eax, ecx
mov     [ebp+var_8], eax
lea     eax, [ebp+Address]
push   eax                ; Address
push   1                  ; UnicodeString
push   83h                ; MbString
push   [ebp+P]           ; P
mov     [ebp+var_64], ecx
call   _xxxSendMessage@16 ; WM_NCCALCSIZE msg
push   dword ptr [ebx+4]
mov     [ebp+var_4], eax
call   _IsStillWindowC@4  ; IsStillWindowC(x)
test   eax, eax
jz     loc_BF88C18A
```

```
cmp     [ebp+var_4], 10h
jl     short loc_BF88BEE3
```

Kaspersky: “In October 2018, our Automatic Exploit Prevention (AEP) systems detected an **attempt to exploit a vulnerability in Microsoft’s Windows operating system**. Further analysis revealed a **zero-day vulnerability** in win32k.sys. The exploit was executed by the first stage of a malware installer in order to gain the necessary privileges for persistence on the victim’s system. So far, we have detected a **very limited number of attacks** using this vulnerability. The **victims are located in the Middle East**.”

... and daily business

Security Bulletins and Advisories

Recent bulletins and advisories



Title	Originally posted	Last updated
APSB19-01 Security updates available for Adobe Flash Player	01/08/2019	01/08/2019
APSB19-02 Security updates available for Adobe Acrobat and Reader	01/03/2019	01/03/2019
APSB18-41 Security updates available for Adobe Acrobat and Reader	12/11/2018	12/11/2018
APSB18-42 Security updates available for Adobe Flash Player	12/05/2018	12/05/2018
APSB18-44 Security updates available for Adobe Flash Player	11/20/2018	11/20/2018
APSB18-43 Security updates available for Adobe Photoshop CC	11/13/2018	11/13/2018
APSB18-40 Security Updates Available for Adobe Acrobat and Reader	11/13/2018	11/13/2018
APSB18-39 Security updates available for Adobe Flash Player	11/13/2018	11/13/2018

Security updates available for Flash Player | APSB18-19

Bulletin ID	Date Published	Priority
APSB18-19	June 7, 2018	1

[APSB18-30 Security updates available for Adobe Acrobat and Reader](#)

10/1/2018

10/1/2018

Dealing with “normal” vulnerabilities

(aka *business as usual*)

Mature organisations:

- harden their configurations
- disable unnecessary products/services
- use more secure alternatives
 - e.g. CERN moved to another PDF reader a few years ago
- apply patches in a timely manner
- **invest in detection (and response)**

This applies also to servers / services

- virtualization & clouds, automatic provisioning, federated identities...

Shadow IT

Internet of
Things

legacy
systems

Internet of Things (in)security

many features
enabled by default

no security built in

remotely accessible,
interconnected



weak default settings
and default passwords

hard or impossible
to patch

Code from 2004, running as *root*

```
foreach my $f (<$_[0]/*.out>){
    [...]
    my $nf="$f.cut";           # files are in /tmp
    system "
        head -100 $f > $nf;
        echo \-----CUT-----\" >> $nf;
        tail -100 $f >> $nf";
```

Two local privilege escalation vulnerabilities:

- **\$f** tainted (name of user-created file, can include shell commands)
- **\$nf** controlled by user (can be a symbolic link to system files)

We often rely on old (and vulnerable) code

... but who knew secure coding back in 2004?

The real target: users

● nikolaos. [redacted]@cern.ch

1 January 2019 at 23:04



nikolaos. [redacted]@cern.ch was under attack! Change your access data!

To: nikolaos. [redacted]@cern.ch

Less ransomware More extortion scams (easier, more effective?)

Hello!

As you may have noticed, I sent you an email from your account.
This means that I have full access to your account.

I've been watching you for a few months now.
The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.
Trojan Virus gives me full access and control over a computer or other device.
This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

Why your antivirus did not detect malware?

Answer: My malware uses the driver, I update its signatures every 4 hours so that your antivirus is silent.

I made a video showing how you satisfy yourself in the left half of the screen, and in the right half you see the video that you watched. With one click of the mouse, I can send this video to all your emails and contacts on social networks. I can also post access to all your e-mail correspondence and messengers that you use.

If you want to prevent this, transfer the amount of \$501 to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin").

My bitcoin address (BTC Wallet) is: 1BPUUNghhuwQjDDvFd3TnJz2ato5dyDLr8

Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best wishes!

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],

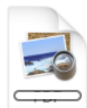
This is safe and secured to access

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.

Scan (1).pdf - Adobe Reader

File Edit View Window Help

Open [Icons] 1 / 1 [Zoom: 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

Convert

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

Adobe Acrobat Secured Document

Security Warning

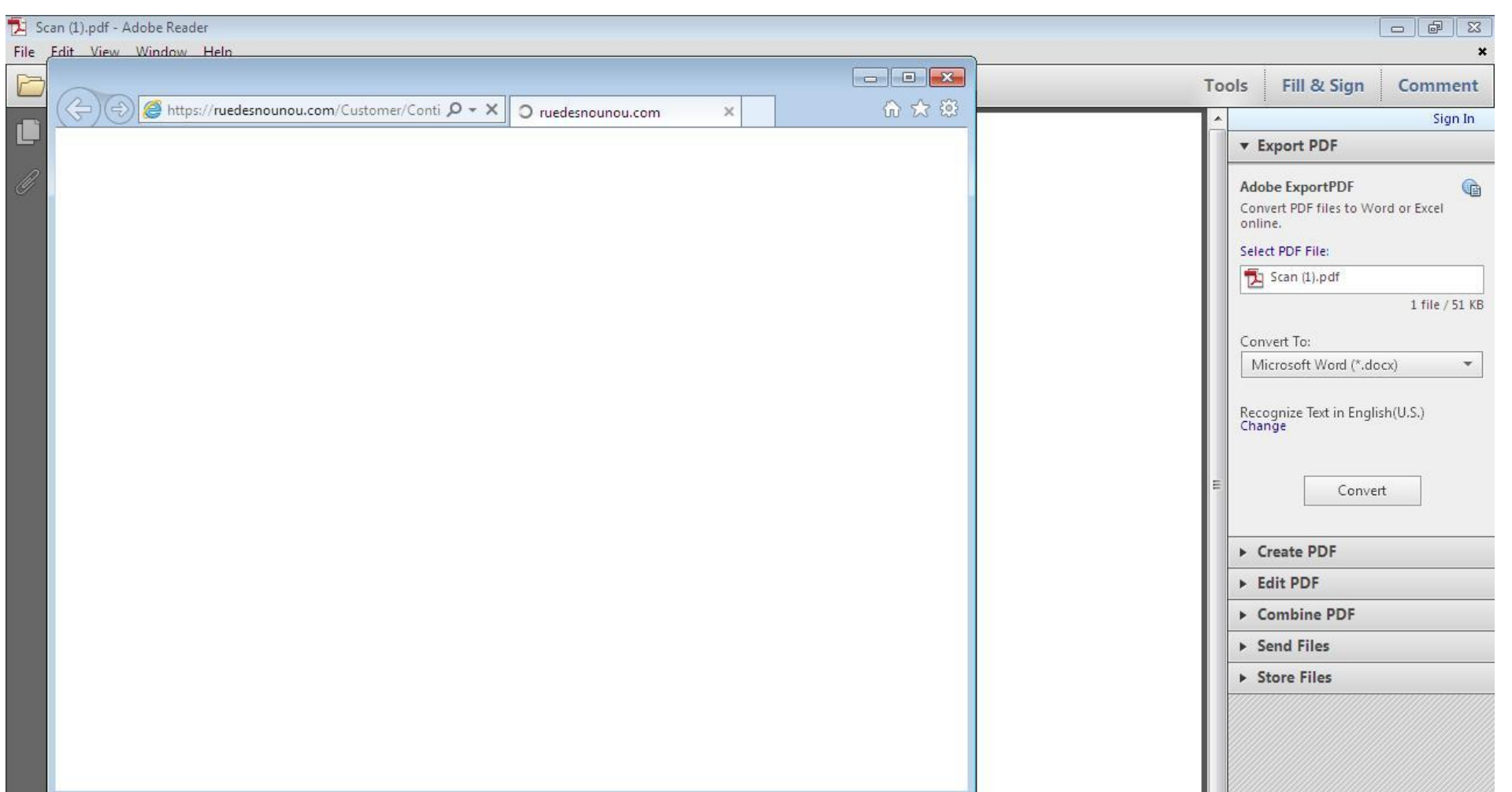


The document is trying to connect to:
<https://ruedesnounou.com>

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](#)



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...

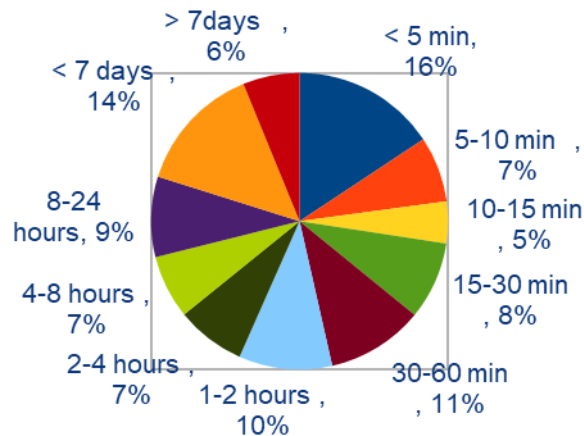
CONFIDENTIAL DOCUMENT

Email attacks

- Email is still the **main attack vector** against organizations and individuals
 - ideal for targeted social engineering attacks
 - particularly hard to control
 - often underestimated (challenges, costs, limitations to protection mechanisms)
- Two attack techniques:
 - **malicious attachment** – protection possible but never 100%
 - **link to a phishing or malware site** – incredibly difficult to protection against
 - (or combined: link in the attachment)
- **User education** and **endpoint protection** are a key line of defense

CERN mailing awareness campaigns

Click rate: 15.3%
(2016: 19.8%; 2017: 18.7%)



"I didn't click, but I forwarded to a colleague, and he clicked to see the page"

Oops... The link you've just clicked is evil!

(Version française ici/en-dessous)

You just fell for a scam. The e-mail whose link you just have clicked is fake. Your "click" could have had severe operational and financial consequences for CERN... Let us explain to you how you can better identify such emails and which consequences clicking on such a malicious link might have for you and your digital assets...

How to identify malicious e-mails

A screenshot of an email interface with several red callout boxes containing questions to help identify malicious emails. The email content is partially visible, showing a subject line "Successful login attempts" and a body with a suspicious link.

Is the sender familiar to you?


Does the sender's name correspond with the shown e-mail-address?

Is the message addressed to you?

Hover your mouse pointer on top. Does the text correspond with the link?

Does the link look reasonable, is not too complex or unreadable?

Does the message concern you? Is it one of your businesses?

Is the message signed ()?

Is the message correctly phrased, without blunt typos, in a language you are able to comprehend?

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 when in doubt.

Conclusions

People and technology ... an unsolvable problem?



