COMPUTER SECURITY UPDATE

LIVIU VÂLSAN
FOR THE CERN COMPUTER SECURITY TEAM

HEPIX AUTUMN 2019, AMSTERDAM

No really big surprises since the last 2 HEPiX meetings
Hence, mostly a resurrection of my and Stefan's slides from
HEPiX Autumn 2018 and HEPiX Spring 2019

PREAMBLE

“Freedom, security, convenience --- choose two” (Dan Geer)

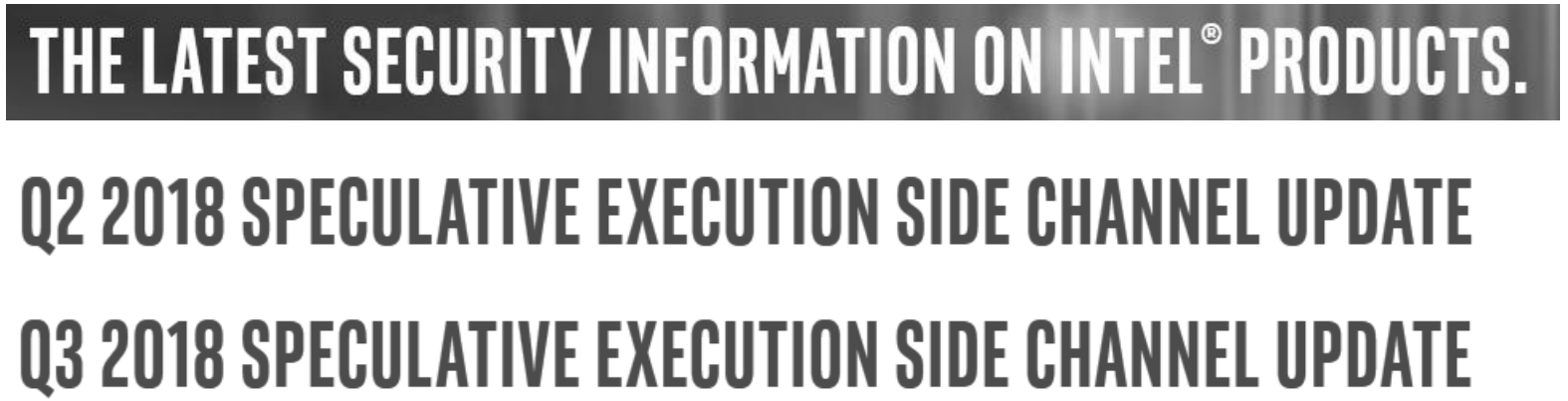
Consequently:

“Security will always be exactly as bad as it can possibly be while allowing everything to still function.”
(Nat Howard)

INTEL SPECULATIVE EXECUTION VULNERABILITIES

- All started in early 2018 with Spectre & Meltdown
  - 3 variants of vulnerabilities

- Since then it became a “tradition”
  - Every quarter a new set of vulnerabilities announced



Q2 2019: MDS INTEL CPU VULNERABILITIES

- Microarchitectural Data Sampling: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091
- 3 different names: RIDL, Fallout, Zombiload
- Same principle as before: abusing CPU level optimizations
  - Relatively hard to exploit in real environments (slow & complex)
- Extra details:
  - CERN Security Advisory
  - Red Hat high level blog post
  - Intel technical deep dive post
  - Every security vulnerability deserves a website, right?

Q2 2019: MDS BROADWELL MICROCODE

- Intel Broadwell-EP (E5-2600 v4) has issues with the microcode update that may lead to a system hang
- Permanent fix: microcode update applied via BIOS update
- In the interim:
  - Force the microcode update at runtime after validating that it doesn't cause system instability
  - Create `/etc/microcode_ctl/ucode_with_caveats/force-early-intel-06-4f-01` and then execute `dracut -f --regenerate-all`

HOW TO CHECK THAT YOUR SYSTEMS ARE PATCHED

- `cat /sys/devices/system/cpu/vulnerabilities/mds`
  - `No such file or directory:` kernel update required
  - `Vulnerable:` Microcode update missing
  - `...,SMT Host State unknown:` VM, check SMT status on the hypervisor
- Debug your CPU/microcode capabilities:
  - https://gitlab.cern.ch/ComputerSecurity/cpuid/raw/master/cpuid.py
  - Check for `MD_CLEAR` in output
  - If not present, check microcode version against Intel CPU list

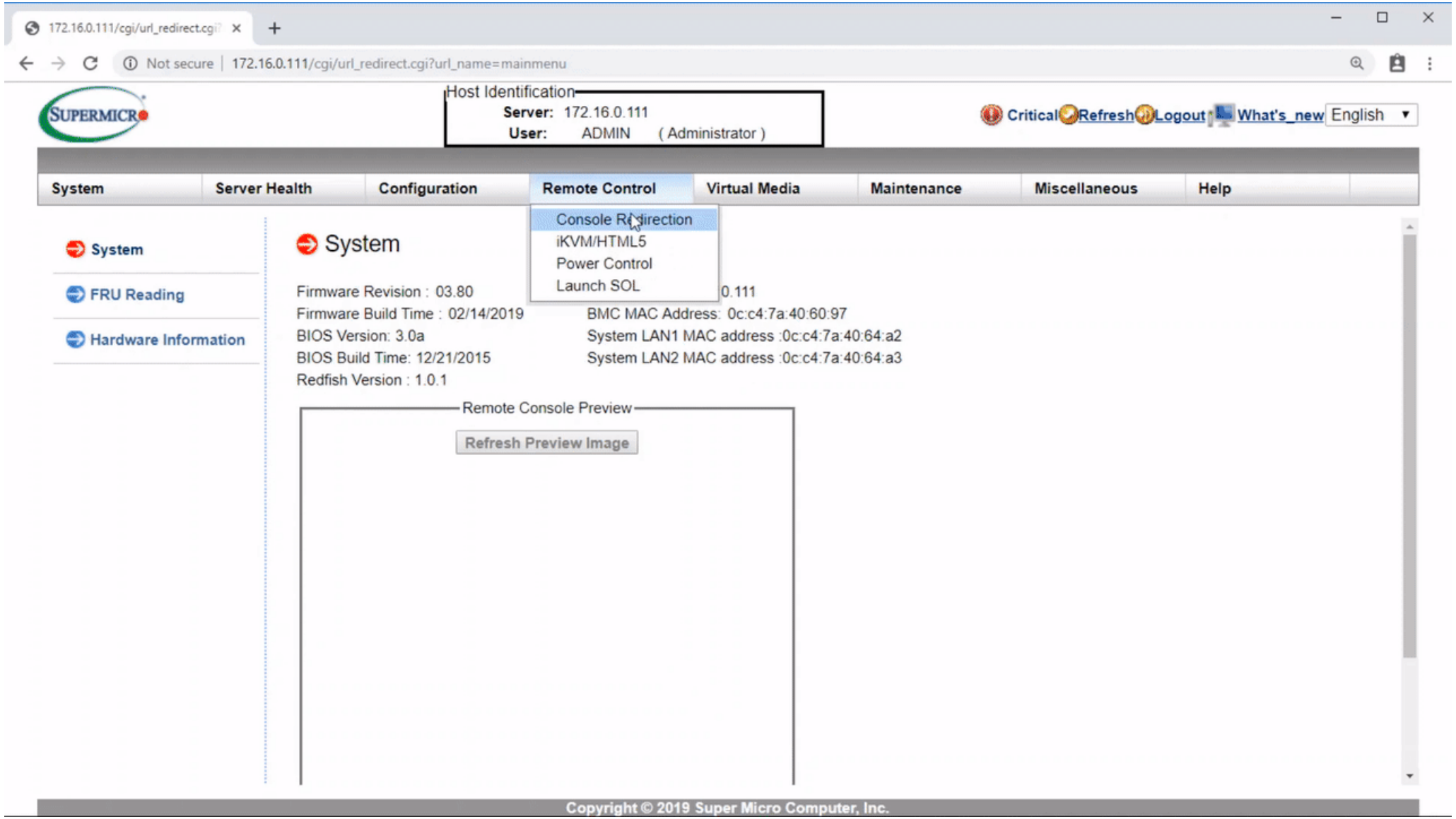
HP iLO Critical Security Vulnerabilities

- Authentication bypass and remote code execution (CVE-2017-12542, CVSSv3 9.8)
  - Affects HP iLO 4
  - Webserver and RedFish REST API abused
  - Fixed in iLO 4 version 2.53 (buggy) and 2.54
- Remote or local code execution (CVE-2018-7078, CVSSv3 7.2)
  - Affects HP iLO 4 and iLO 5
  - Fixed in iLO4 versions 2.60 (released in May 2018)
  - Fixed in iLO5 versions 1.30 (released in June 2018)
- Discovered by Airbus security: presentation, toolbox

SUPERMICRO VIRTUAL MEDIA SECURITY VULNERABILITIES

- Supermicro H11, H12, M11, X9, X10 and X11 affected by multiple encryption and authentication issues
  - CVE-2019-16649, CVE-2019-16650
- Capturing of BMC credentials and data transferred over virtual media devices
- Attackers can connect virtual USB devices to the server managed by the BMC
- More details available from Eclypsium and Supermicro

SUPERMICRO VIRTUAL MEDIA SECURITY VULNERABILITY



BMC VULNERABILITIES: MITIGATIONS

- Update firmware to the latest version
- Disable unnecessary services
- Disable / block access to unused ports
- Isolate BMCs (IPMI interfaces)
  - Dedicated physical interface
  - Private IPs, no Internet connectivity
  - Dedicated network domain / VLAN
- Change default credentials

Increased Sophistication

From: Giovanni [redacted] <office.outlook@yandex.com>
Date: Monday, 10 December 2018 at 10:28
To: [redacted]
Cc: [redacted]

Subject: Giovanni [redacted] has shared a file with you

Please see the attached for your action

Regards
Giovanni [redacted]

Scan.pdf

10.12.2018, 20:37, [redacted]

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

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]

SIX MONTHS 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

AFTER ANOTHER FOUR MONTHS...

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]

BEWARE OF BUSINESS EMAIL COMPROMISE

From: Mustafa <mustafa@mavi com.tr<mailto:mustafa@mavi com.tr>>
Sent: 29 July 2019 07:22
To: Riad <riad.@cern.ch<mailto:riad.@cern.ch>>
Cc: David <David.@cern.ch<mailto:David.@cern.ch>>; Gaelle <gaelle.@cern.ch<mailto:gaelle.@cern.ch>>;
Sani M Adam <sales2@mavi-tr.com<mailto:sales2@mavi-tr.com>>
Subject: Request_of_payment _N °8515905205028 _ _MAVI _

Dear Mr. ,

Did you transfer the payment as advised?
Please kindly email us the swift copy of payment asap.

İyi Çalışmalar.

Mustafa
Genel Müdür

MAVİ .LTD.ŞTİ.

Tel :+90
Fax :+90
www.mavi .com.tr<http://www.mavi .com.tr/>
www.mavi .com.tr<http://www.mavi .com.tr/>

BEWARE OF BUSINESS EMAIL COMPROMISE

From: Riad <riad.@cern.ch<mailto:riad.@cern.ch>>
Sent: 29 July 2019 07:27
To: Mustafa <mustafa@mavi-tr.com<mailto:mustafa@mavi-tr.com>>
Cc: CERN Treasury <Cern.Treasury.@cern.ch<mailto:Cern.Treasury.@cern.ch>>; David
<David.@cern.ch<mailto:David.@cern.ch>>; Gaelle <gaelle.@cern.ch<mailto:gaelle.@cern.ch>>; Sani M Adam
<sales2@mavi-tr.com<mailto:sales2@mavi-tr.com>>
Subject: RE: Request_of_payment _N °8515905205028 __MAVI_

Dear Mr. ,

The payment is in progress. The bank transfer should be executed within 7 open days at latest.

We will send you a proof of payment when it will be done.

Best regards,

Riad
CERN - European Organization for Nuclear Research
Finance and Administrative Processes Department
Accounting Payables Service (FAP-ACC-AP)
CH - 1211 GENEVA 23
Tel : (+41)
riad.@cern.ch<mailto:riad.@cern.ch>

BEWARE OF BUSINESS EMAIL COMPROMISE

On Mon, Jul 29, 2019 at 10:25 AM CERN Treasury <Cern.Treasury.@cern.ch<mailto:Cern.Treasury.@cern.ch>> wrote:
Dear all,

It seems that the bank details are different than the ones used by us for the last payment to your company in January.

Can we please kindly ask you to fill in the attached form and to send it back to us ?

We need to receive the confirmation before tomorrow morning in order for you to receive the funds before the end of the week.
Thank you in advance,
Kind regard
Hugo
CERN Treasury & Payments

BEWARE OF BUSINESS EMAIL COMPROMISE

From: Mustafa <mustafa @mavi .com.tr>
Sent: lundi, 29 juillet 2019 13:05
To: Riad <riad. @cern.ch>; CERN Treasury <Cern.Treasury. @cern.ch>
Cc: CERN Treasury <Cern.Treasury. @cern.ch>; David <David. @cern.ch>; Gaelle <gaelle. @cern.ch>; Sani M Adam <sales2@mavi -tr.com>
Subject: RE: Request_of_payment _N °8515905205028 _

Dear Mr. Hugo,

Please find attached.
Await your swift copy of payment.

İyi Çalışmalar.

Mustafa
Genel Müdür

BEWARE OF BUSINESS EMAIL COMPROMISE

Whois Record for Mavi[redacted].com.tr

Domain Profile

Registrant Org	Mavi[redacted]
Registrant Country	tr
Registrar Status	
Dates	3,374 days old Created on 2010[redacted] Expires on 2021-[redacted]
Name Servers	NS11.[redacted] (has 1,491 domains) NS12.[redacted] (has 1,491 domains)
Tech Contact	–
IP Address	94.102.[redacted] - 282 other sites hosted on this server
IP Location	- Denizli - Denizli - Netinternet Bilisim Teknolojileri As
ASN	AS51559 NETINTERNET Netinternet Bilisim Teknolojileri AS, TR (registered [redacted] 2010)
Hosting History	1 change on 2 unique name servers over 5 years

Website

Website Title	None given.
Terms	1,658 (Unique: 870, Linked: 57)
Images	31 (Alt tags missing: 0)
Links	62 (Internal: 49, Outbound: 3)

BEWARE OF BUSINESS EMAIL COMPROMISE

Whois Record for Mavi[redacted]-tr.com

Domain Profile

IP Address	64.20[redacted] - 785 other sites hosted on this server
IP Location	- New Jersey - Secaucus - Interserver Inc
ASN	AS19318 IS-AS-1 - Interserver, Inc, US (registered Dec 09, 2005)
Domain Status	Registered And Active Website
IP History	1 change on 1 unique IP addresses over 0 years
Registrar History	1 registrar
Hosting History	1 change on 2 unique name servers over 0 year

Website

Website Title	Index of /
Server Type	LiteSpeed
Response Code	200
Terms	23 (Unique: 23, Linked: 6)
Images	2 (Alt tags missing: 0)
Links	5 (Internal: 5, Outbound: 0)

HOW TO (TRY) TO PROTECT YOURSELF AGAINST BEC

- Security awareness is key
  - The from email address is not to be trusted
  - Check the reply-to address
- Monitor your domain for typosquatting attacks
  - The dnstwist domain name permutation tool can help similar-looking domains that adversaries can use to attack you

TWIST THAT DNS DOMAIN NAME

```
dnstwist 1.02b by <marcin@ulikowski.pl>

usage: ./dnstwist.py [OPTION]... DOMAIN

Find similar-looking domain names that adversaries can use to attack you. Can
detect typosquatters, phishing attacks, fraud and corporate espionage. Useful
as an additional source of targeted threat intelligence.

positional arguments:
  domain                domain name or URL to check

optional arguments:
  -h, --help            show this help message and exit
  -c, --csv             print output in CSV format
  -j, --json            print output in JSON format
  -r, --registered      show only registered domain names
  -w, --whois           perform lookup for WHOIS creation/update time (slow)
  -g, --geoip           perform lookup for GeoIP location
  -b, --banners         determine HTTP and SMTP service banners
  -s, --ssdeep          fetch web pages and compare their fuzzy hashes to
                        evaluate similarity
  -m, --mxcheck         check if MX host can be used to intercept e-mails
  -d FILE, --dictionary FILE
                        generate additional domains using dictionary FILE
  -t NUMBER, --threads NUMBER
                        start specified NUMBER of threads (default: 10)
elceef@osiris:~/dnstwist$
```

https://github.com/elceef/dnstwist

MALWARE IN REPLIES TO EXISTING EMAIL THREADS

From: info@hotelariston.com <info@hno-orl-weinfelden.ch>
To: Melissa <melissa. @cern.ch>
Subject: RE: school confirmation- authorization of credit card.
Date: Mon, 14 Oct 2019 18:15:28 +0530 (*14/10/19 14:45:28*)

mit dieser E-Mail schicke ich Euch zwei wichtige Dokumente.

info@hotelariston.cominfo@hotelariston.com

Hello,

Please find attached my form and relevant documents. Please let me know if I'm missing any information.

Thank you,

Melissa

From: info@hotelariston.com [info@hotelariston.com]
Sent: 27 April 2019 18:29
To: Melissa
Subject: R: INFN school confirmation- authorization of credit card.

DISABLE THE LOADING OF REMOTE CONTENT

Welcome dear Dr. Daniel [redacted],

My real name is Gabor Fekete. The Gabriel Black is only a direct translation of my hungarian name. You know very-well me. I sent you many emails with spoofed senders in the headers of that emails. But not this is the important. The important things are found in the followings.

In 2017 the physics Nobel Committee that is the world's pseudo-scientist mafia again donated Nobel prizes to three pseudo-scientists for the detection of the invented and non-existent gravitational wave idiocy which allegedly consists of time and space.

The time is not part of the real world, it is only a human invention and exists only in man's mind as imagination. Neither the pointing clock nor the atomic clock does not measure any time, only the same vibration phases are counted. That is why the faster vibration clock counts more identical vibration phases than its slower vibrating companion. The big pointer counts the identical vibration phases of the seconds pointer and the small pointer counts the identical vibration phases of the big pointer. For this reason the atomic clock nor accurate, since it how would be accurate if it does not measure anything only counts the same vibration phases. The non-existent time does not go anywhere, does not slowing, does not dilatation, have not the feature of the force, only the clocks vibrate, the Earth spins around its axis and circles around the sun. These periodical movements generate the imagination of time in mind of the man. The stupid Einstein, the Nobel awarded fool and pseudo-scientist Thorne, Barish and Weiss and the Nobel donor pseudo-scientist mafioso Alexander Skrinsky did not know this.

DO NOT ALLOW LOADING OF REMOTE CONTENT

My emails which were sent to you with spoofed sender headers have been read 13 times on the following IP address(es), since 08.08.2016.

Reading data of Daniel [redacted] <daniel.[redacted]@cern.ch>

	IP address	Host of IP	Has been read	Geo Location	Sent	The "Sender" was
1	184.65.[redacted]	[redacted].net	2016-08-08/16:24:42	Canada	160808	
2	128.141.[redacted]	cern.ch	2016-08-31/10:13:12	Switzerland/Geneva	160831	
3	128.141.[redacted]	cern.ch	2016-09-05/11:36:27	Switzerland/Geneva	160905	
4	128.141.[redacted]	cern.ch	2016-09-05/15:26:34	Switzerland/Geneva	160905	
5	128.141.[redacted]	cern.ch	2016-10-19/09:21:15	Switzerland/Geneva	161019	
6	128.141.[redacted]	cern.ch	2016-10-20/11:03:34	Switzerland/Geneva	161020	
7	128.141.[redacted]	cern.ch	2017-01-17/16:03:45	Switzerland/Geneva	170117	
8	128.141.[redacted]	cern.ch	2017-01-31/09:29:07	Switzerland/Geneva	170131	
9	194.12.[redacted]	cern.ch	2017-02-06/11:52:18	Switzerland/Geneva	170206	
10	128.141.[redacted]	cern.ch	2017-02-09/15:07:45	Switzerland/Geneva	170209	
11	194.12.[redacted]	cern.ch	2017-02-17/10:36:25	Switzerland/Geneva	170217	
12	128.141.[redacted]	cern.ch	2017-03-28/15:56:03	Switzerland/Geneva	170328	
13	194.12.[redacted]	cern.ch	2018-01-16/09:16:55	Switzerland/Geneva	180116	

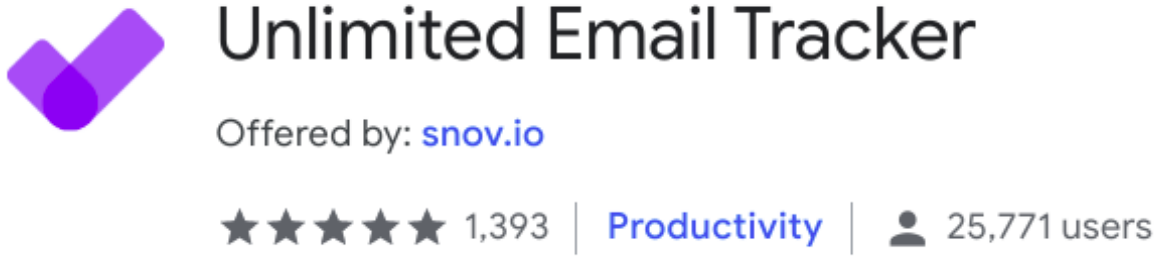
The timezone of the readings is Europe/Paris. The date format is Year-Month-Day. The reading data of you and further 41.000 persons are public on my site below.

APT ACTORS USE THE SAME TECHNIQUES

- Usually for reconnaissance purposes
- Charming Kitten APT actor actively targeting academic researchers
- Making use of Google Chrome extension for email tracking

SHADY CHROME EXTENSION FOR GMAIL TRACKING

- Available in the official Google Web Store
- 25k installs, 4.9 review score from 1400 reviews
- *Free email tracker extension for your Gmail. Email tracking and link clicks statistics for your email messages.*



GLOBAL PHISHING CAMPAIGNS AGAINST UNIVERSITIES

- In March 2018, a phishing campaign against universities became known under the name "Silent Librarian“
  - Attributed to an Iranian-based actor
  - Campaign was mainly run during 2017
- In August 2018, a new, similar phishing campaign was identified, dubbed “Cobalt Dickens”
- Upon entering the credentials on the phishing site, the user gets redirected to the real site, already logged in.
- Universities' online library systems being targeted

NOT THE ONLY APT TARGETING ACADEMIA

- COBALT DICKENS goes back to school… again
- New campaign during summer of 2019 using compromised university resources to send library-themed phishing emails
- Recipients who click on the link are directed to a web page that looks identical or similar to the spoofed library resource
- The victim's browser is sent to the legitimate site after credentials are captured

IT ALL STARTS WITH AN EMAIL

From Library Services [redacted]
Subject **Library Services** 8/2/19, 3:11 AM
To [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

You may now log in by clicking this link or copying and pasting it into your browser. A successful login will activate your account and you will be redirected to your page:

[redacted]libe.cf/[redacted]gin/pages/login.jsp

This link can only be used once to log in and will lead you to a page where you can see your profile.

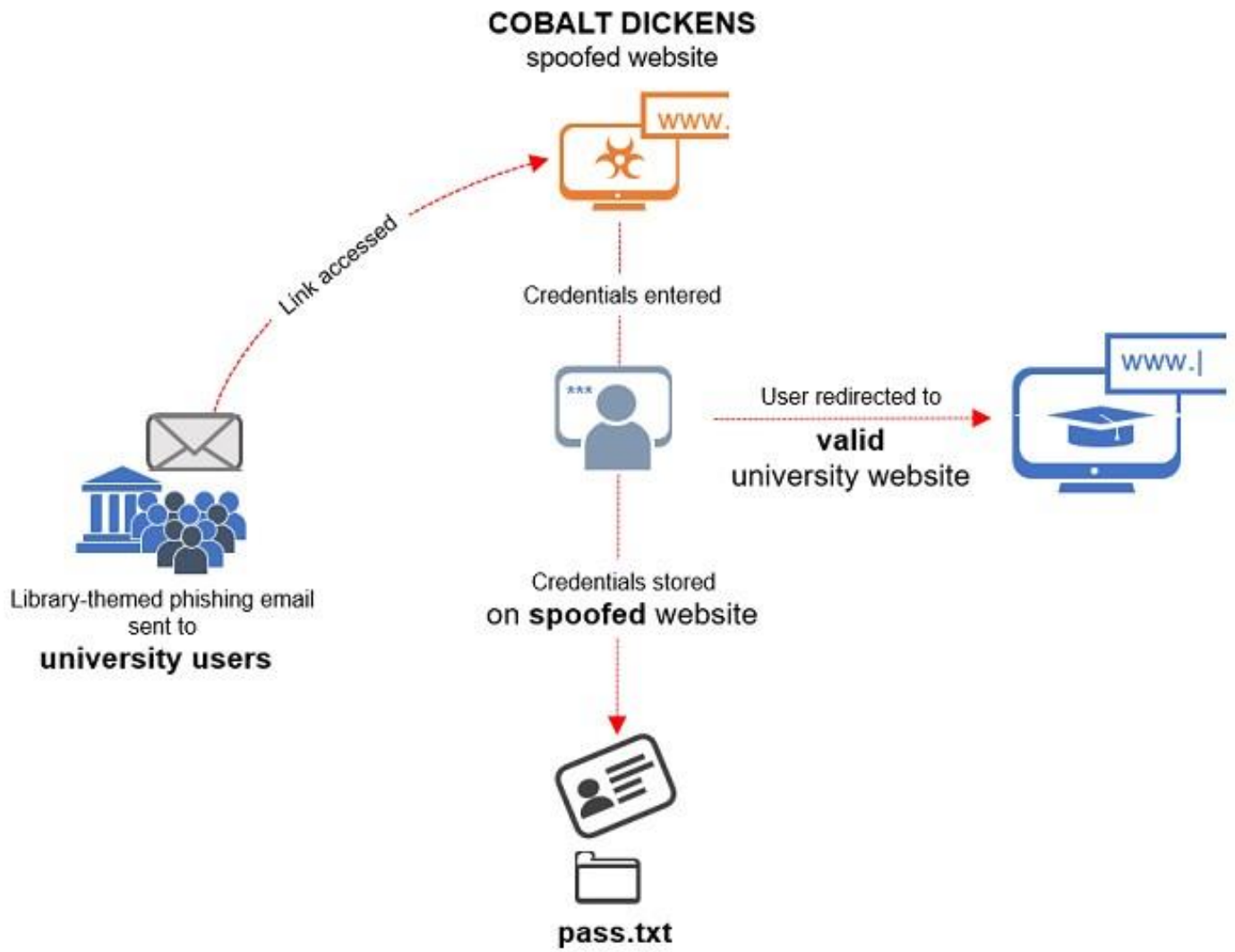
After doing that, you will be able to log in at library.

Sincerely,

[redacted]

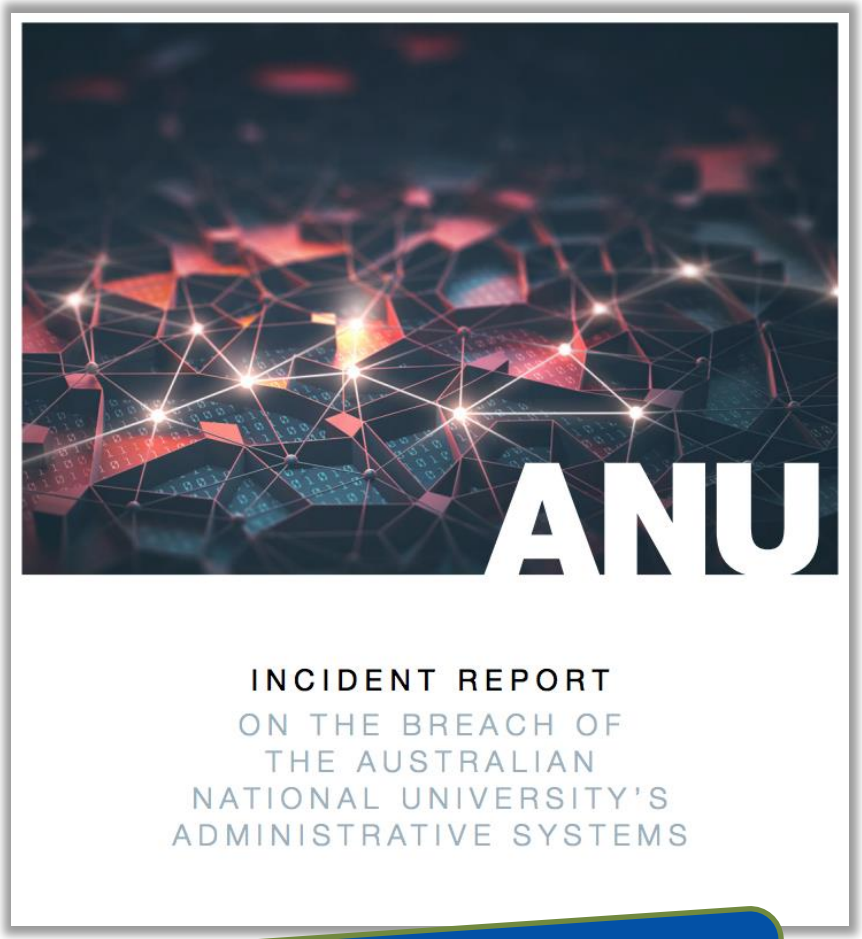
https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

AND THIS IS WHAT HAPPENS NEXT



https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

A RECENT DATA BREACH AT ANU



Kudos for being transparent!

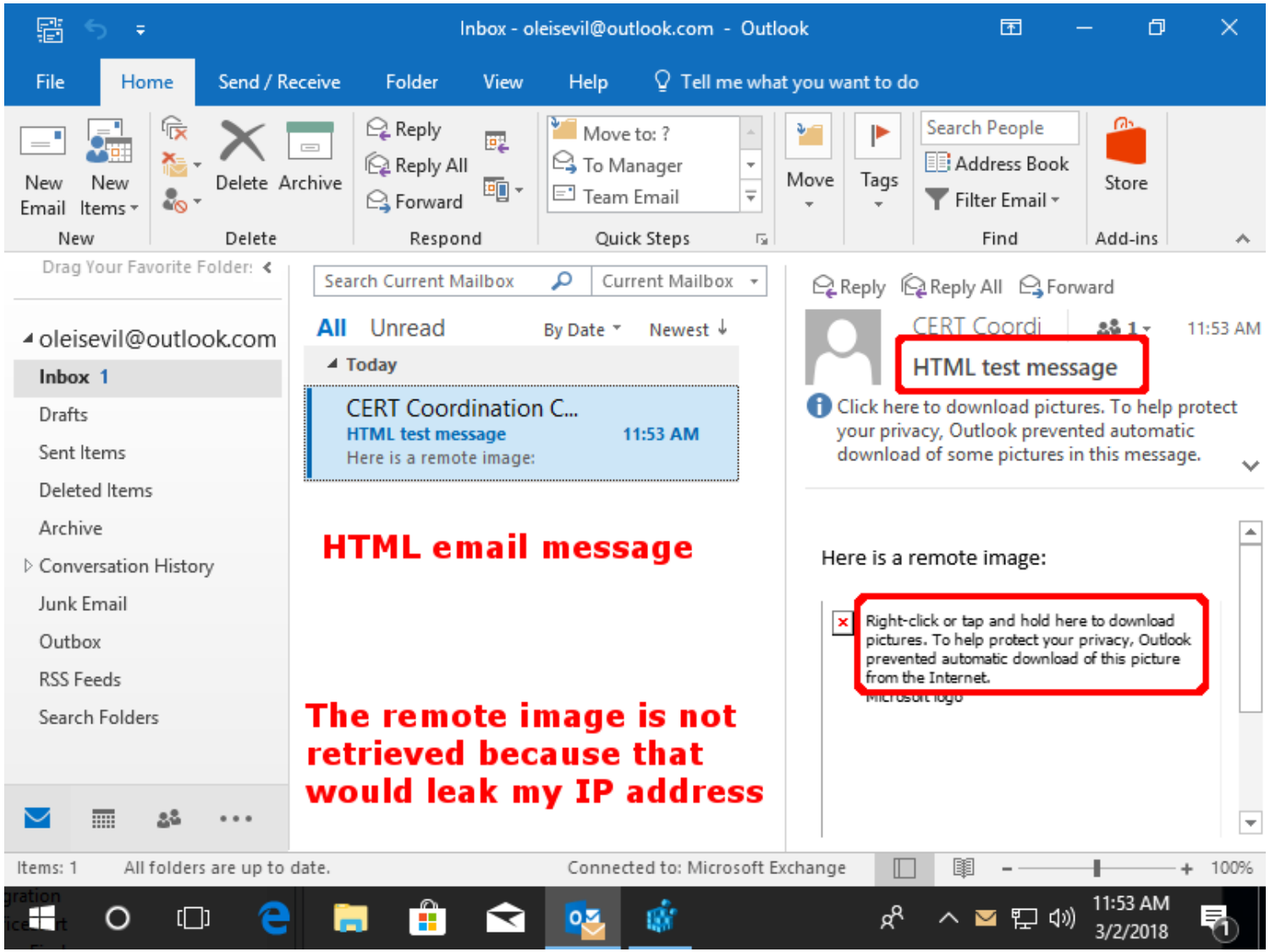
Public detailed report (Oct. 2nd, 2019)

*"The initial means of infection was a sophisticated **spearphishing email** (targeting a senior staff member) which did not require user interaction, ie clicking on a link or downloading an attachment.*

The credentials taken from this account were used to gain access to other systems.

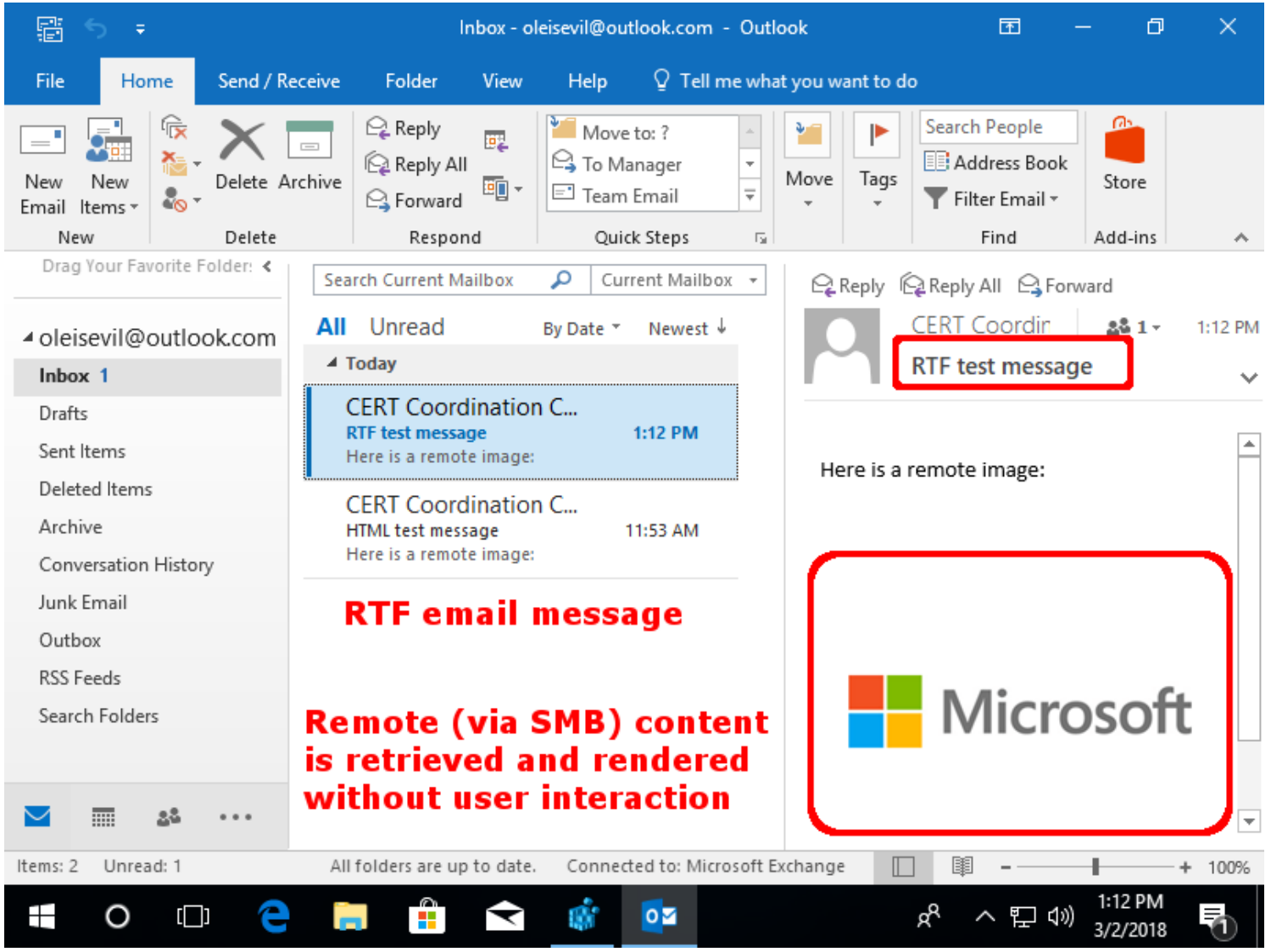
Information from victim's calendar was used to conduct additional spearphishing attacks later in the campaign."

THIS IS HOW MICROSOFT OUTLOOK SHOULD BEHAVE



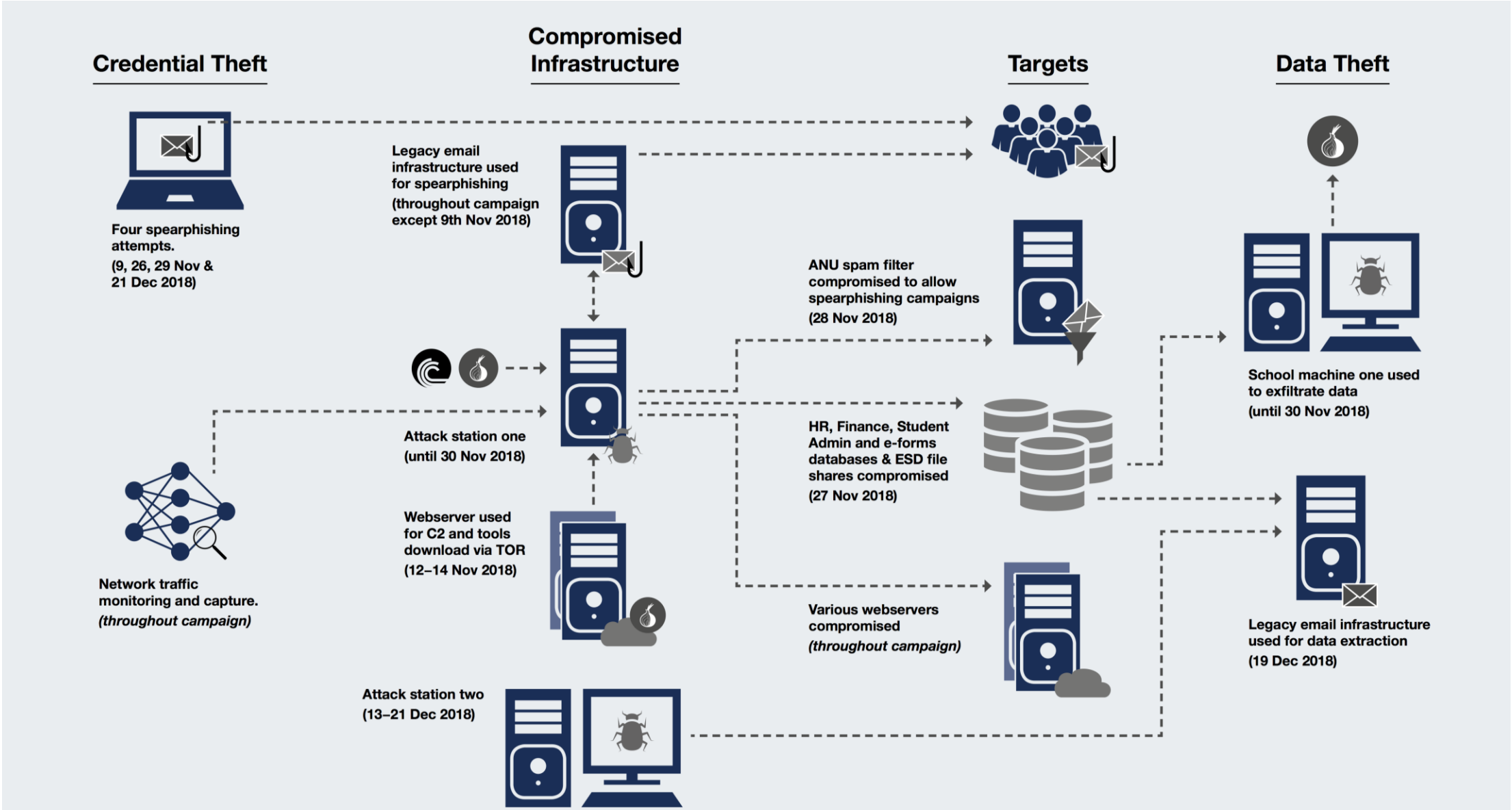
https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

BUT IN THE CASE OF AN RTF EMAIL…

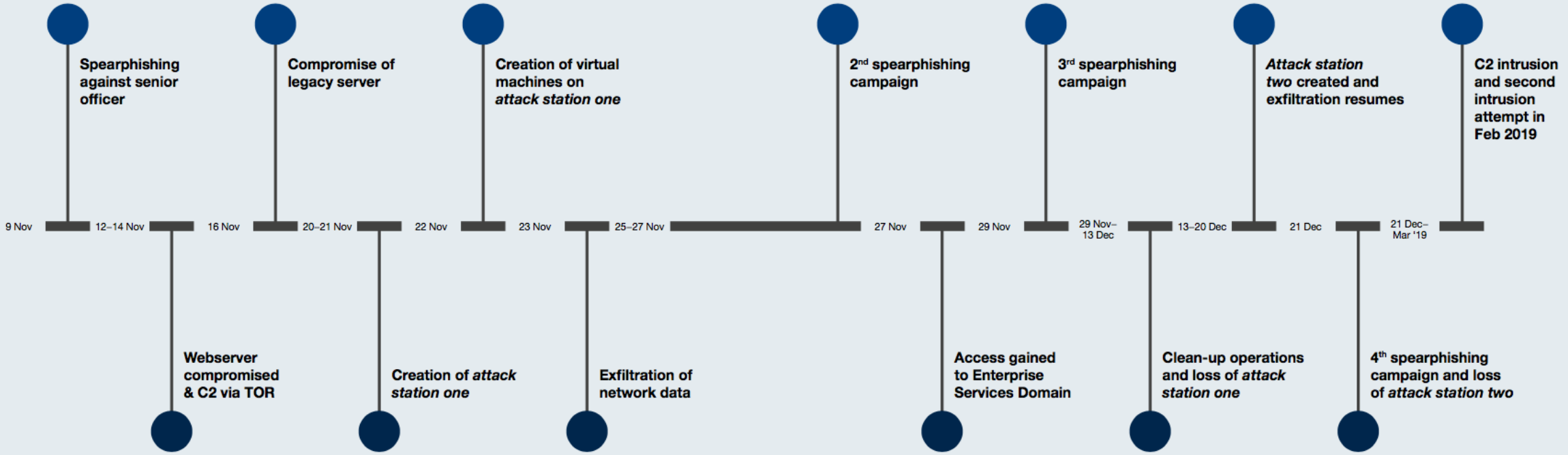


https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

LATERAL MOVEMENTS, STEALTHY DATA EXFILTRATION



TIMELINE


9 Nov
Spearphishing against senior officer
12–14 Nov
Webserver compromised & C2 via TOR
16 Nov
Compromise of legacy server
20–21 Nov
Creation of *attack station one*
22 Nov
Creation of virtual machines on *attack station one*
23 Nov
25–27 Nov
Exfiltration of network data
27 Nov
2nd spearphishing campaign
29 Nov
Access gained to Enterprise Services Domain
29 Nov–13 Dec
3rd spearphishing campaign
13–20 Dec
Clean-up operations and loss of *attack station one*
21 Dec
Attack station two created and exfiltration resumes
21 Dec–Mar '19
4th spearphishing campaign and loss of *attack station two*
C2 intrusion and second intrusion attempt in Feb 2019

HOW TO PROTECT YOURSELF AND YOUR INSTITUTE

- Disable loading of remote content in your email client
- Keep your system up to date
  - RTF email vulnerability (CVE-2018-0950) patched in October 2018
- If possible block outgoing SMB connections

SEEMINGLY ENDLESS STRING OF DATA LEAKS

- We are seeing an almost seemingly endless string of data breaches
- 34 data leaks made public since last HEPiX
  - More than 500 million leaked items (credentials or disclosure of personal information)
- Credential stuffing attacks becoming increasingly popular

(2019/1) BigDB & Collection #1-5

HACKING | By Lorenzo Franceschi-Bicchierai | Jan 17 2019, 6:16pm

The 'Biggest EVER' Collection of Hacked Passwords Is Not That Bad

Someone put together a massive list of 773 million unique email addresses and 21 million unique passwords. But there's really no reason to panic.

MOTHERBOARD

- Most recent dump-of-dumps with lots of juicy stuff
- …of course not all critical. "12345" can be a useful token…
- Can you be sure passwords are not reused???
- CERN informed:
  - 2751 staff & users of their CERN or external email addresses being exposed
  - Plus 236 affiliated universities, institutes & partner-companies
  - Want to join? Please talk to me!

https://motherboard.vice.com/en_us/article/evegxw/collection-one-data-breach-password-hack-what-to-do

DATA BREACHES ARE CONTINUING AT AN ALARMING PACE

- A total of 59 data breaches totalling 735 million compromised accounts uploaded to HaveIBeenPwned since the last HEPiX meeting
- Our community actively targeted by credential spray attacks
- Subscribe to notifications from HaveIBeenPwned
- CERN can also send you notifications of leaked credentials
- Integrate HaveIBeenPwned leaked passwords in your password change workflow
- Implement 2FA

(2018/9) Facebook, again…

PCMag UK | News & Analysis | News

Facebook Targets Ads Using Phone Numbers Provided for 2FA

BY ADAM SMITH 28 SEP 2018, 7:41 P.M.

Facebook lets advertisers upload information about people they want to target, and matches that information to numbers and emails it has in its database. That includes phone numbers provided for two-factor authentication and information pulled from friends' address books.

0 SHARES

Facebook has confirmed that mobile numbers submitted to the site for the purposes of two-factor authentication (2FA), as well as contact information pulled from friends' address books, have been used to target ads.

BBC Sign in News Sport Weather Shop Reel Travel Mo

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

Millions of Facebook passwords exposed internally

21 March 2019 Share

The passwords of millions of Facebook users were accessible by up to 20,000 employees of the social network, it has been reported.

Security researcher **Brian Krebs broke the news about data protection failures**, which saw up to 600 million passwords stored in plain text.

TWITTER 2FA

SECURITY FAUX PAS —

Twitter transgression proves why its flawed 2FA system is such a privacy trap

Twitter 2FA is every bit as bad as critics said it was. Site signals a change is coming.

DAN GOODIN - 10/9/2019, 2:30 AM

Enlarge

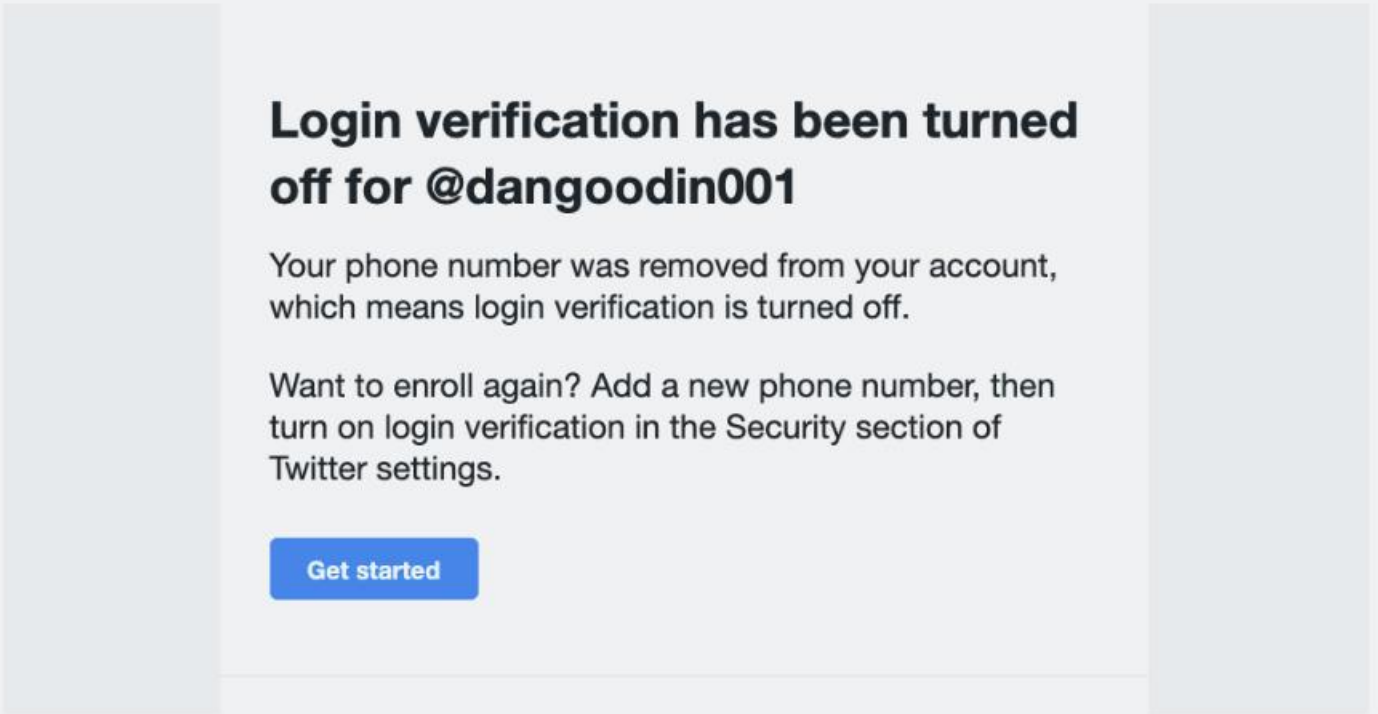
146

If ever there was a surefire way to sour users against a two-factor authentication system that was already highly flawed, Twitter has found it. On Tuesday, the social media site said that it used phone numbers and email addresses provided for 2FA protection to tailor ads to users.

https://arstechnica.com/information-technology/2019/10/twitter-used-phone-numbers-provided-for-2fa-to-match-users-to-advertisers/

TWITTER 2FA

Twitter requires users to provide a valid phone number to be eligible for 2FA protection. A working cell phone number is mandatory even when users' 2FA protection is based solely on security keys or authenticator apps, which don't rely on phone numbers to work. Deleting a phone number from a user's Twitter settings immediately withdraws an account from Twitter 2FA, as I confirmed just prior to publishing this post.



https://arstechnica.com/information-technology/2019/10/twitter-used-phone-numbers-provided-for-2fa-to-match-users-to-advertisers/

2FA RECOMMENDATIONS

- Use 2FA whenever possible
- Do not use SMS for 2FA whenever possible
- Sim swap attacks are far too common
- In fact do not rely on SMS for anything sensitive
- Prefer other means of 2FA (e.g. Authenticator App, Yubikey) whenever possible; prefer redundancy
- Safely store 2FA recovery codes

DNS-OVER-HTTPS IS COMING TO A BROWSER NEAR YOU

- Mozilla announced that

We plan to gradually roll out DoH in the USA starting in late September. Our plan is to start slowly enabling DoH for a small percentage of users while monitoring for any issues before enabling for a larger audience. If this goes well, we will let you know when we're ready for 100% deployment.

https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

DNS-OVER-HTTPS IS COMING TO A BROWSER NEAR YOU

- Google is taking a more conservative approach

*...this would **upgrade the protocol** used for DNS resolution **while keeping the user's DNS provider unchanged**. It's also important to note that DNS over HTTPS does not preclude its operator from offering features such as family-safe filtering.*

We are aiming for an experiment in Chrome 78 (branch cut: Sept 5th; estimated Stable: Oct 22nd) followed by a launch if everything goes well.

https://www.chromium.org/developers/dns-over-https

DNS-OVER-HTTPS

- In theory DNS-over-HTTPS is a good step towards preserving user privacy
  - Many DoH services are operated by corporations already controlling a significant proportion of Internet traffic
- With DoH (and TLS 1.3) we are losing ever more visibility into the network traffic
  - We may not be able to provide the same level of protection to our users going forward
  - On the other hand we already see malware making use of DoH already

DNS-OVER-HTTPS

- Determine whether you want to allow, discourage, or disallow use of alternative DoH recursive resolvers at your institution
- If you decide to discourage or disallow the usage of DoH:
  - Configure your DNS server to return NXDOMAIN for A and AAAA records for the use-application-dns.net canary domain
  - DoH is bootstrapped via the OS DNS so you could try to block resolution of popular DoH servers (not recommended)
- Communicate with your users

CONCLUSIONS AND RECOMMENDATIONS

If we want to ~~**win**~~**/keep up with this marathon**, we should/must(!)

- More often **choose "security"** instead of "convenience"
- More often **consider "privacy"** instead of "freedom";
- Have deep direct **ties with the community** to learn quickly about the malicious evil (and where they affect / attack us);
- Have good **traceability & logging** in place to figure out where we are attacked / affected;
- Have good configuration management for **prompt and agile patching** (office computing, data centre *and* control systems);
- Accept that we do not and cannot control the full phase-space. Protection is often difficult/impossible, and - for sure - costly.


CERN