CONTEMPORARY NEWS

WEEK 13 OF THE COURSE

Disclaimer: Not as (this week) recent as usually

It is back from august

KNOB ATTACK

KNOB Attack

Key Negotiation of Bluetooth Attack: Breaking Bluetooth Security

KEY NEGOTIATION OF BLUETOOTH ATTACK: BREAKING BLUETOOTH SECURITY

- Bluetooth uses custom security mechanisms (at the link layer)
  - Open but complex specification
  - No public reference implementation

KEY NEGOTIATION OF BLUETOOTH ATTACK: BREAKING BLUETOOTH SECURITY

- Paired devices negotiate an encryption (K'*c*) key upon connection
- Bluetooth allows K'*c* with 1 byte of entropy and does not authenticate Entropy Negotiation
- **Key Negotiation of Bluetooth (KNOB) attack** sets N=1, and brute forces K'*c*
  - Eavesdrop the ciphertext and brute force the key in real time

SEVERITY

- Affects any standard compliant Bluetooth device (architectural attack)
- Allows to decrypt all traffic and inject valid traffic

RESOURCES

- https://knobattack.com/
- https://francozappa.github.io/publication/knob/slides.pdf
- https://www.version2.dk/artikel/kasper-opdagede-sikkerhedshul-bluetooth-princippet-kunne-man-angribe-kilometers-afstand (In danish)

WEEK 12 OF THE COURSE

THIS WEEK - A SURVEY

- New Unpatched Strandhogg Android Vulnerability Actively Exploited in the Wild
- Europol Shuts Down 'Imminent Monitor' RAT Operations With 13 Arrests
- Magento Marketplace Suffers Data Breach Exposing Users' Account Info
- Over 12,000 Google Users Hit by Government Hackers in 3rd Quarter of 2019
- Latest Kali Linux OS Added Windows-Style Undercover Theme for Hackers

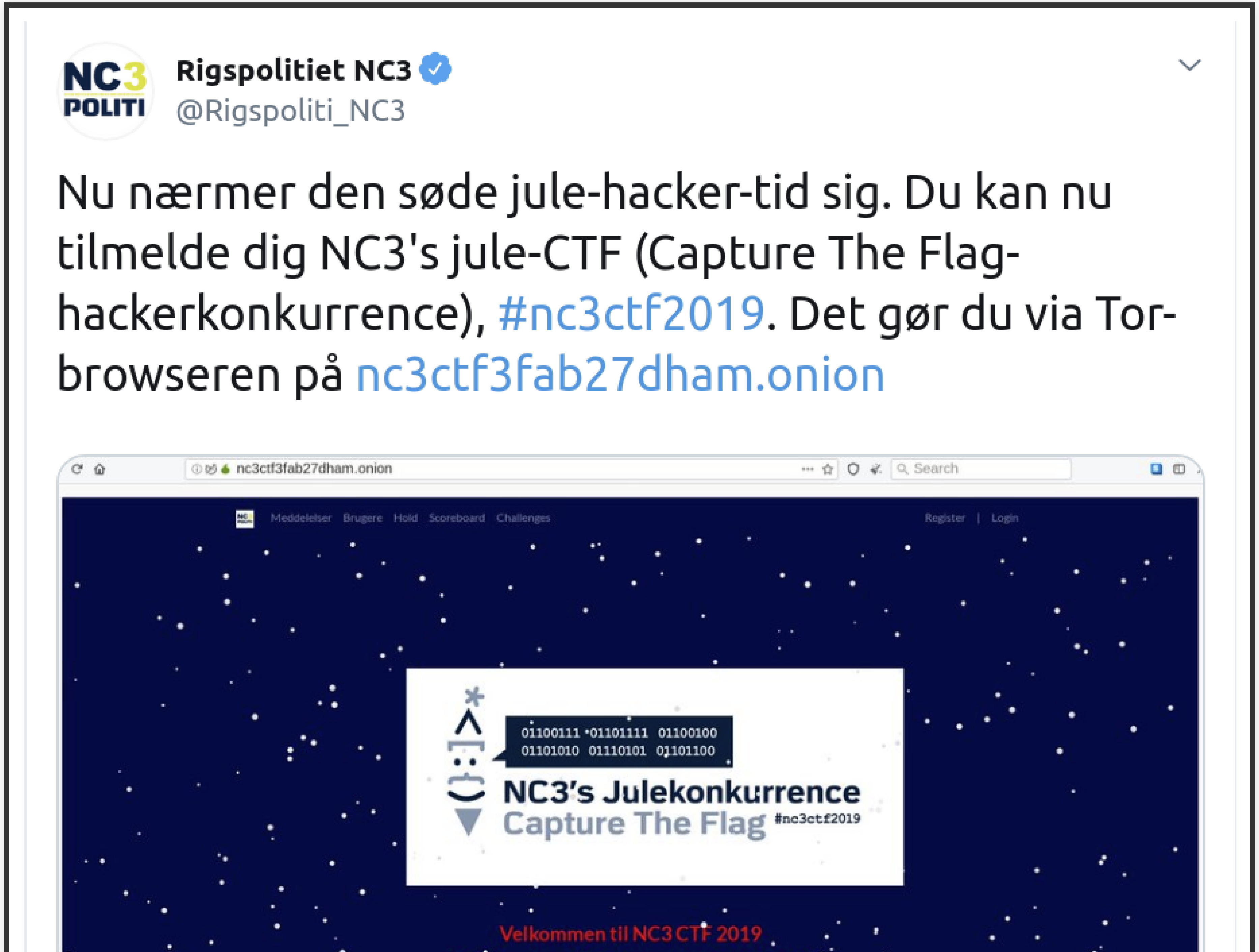
LINKS

- https://thehackernews.com/2019/12/strandhogg-android-vulnerability.html
- https://thehackernews.com/2019/11/europol-imminent-monitor-rat.html
- https://thehackernews.com/2019/11/magento-marketplace-data-breach.html
- https://thehackernews.com/2019/11/google-government-hacking.html
- https://thehackernews.com/2019/11/kali-linux-undercover-mode.html

RIGSPOLITIET NC3

National Cyber Crime Center (NC3) is the danish national police’s center for cyber-crime.

RIGSPOLITIET NC3



Rigspolitiet NC3
@Rigspoliti_NC3

Nu nærmer den søde jule-hacker-tid sig. Du kan nu tilmelde dig NC3's jule-CTF (Capture The Flag-hackerkonkurrence), #nc3ctf2019. Det gør du via Tor-browseren på nc3ctf3fab27dham.onion

01100111 01101111 01100100
01101010 01110101 01101100

NC3's Julekonkurrence
Capture The Flag #nc3ctf2019

Velkommen til NC3 CTF 2019

Fra: Torsdag den 28. november 2019 kl. 10

Til: Torsdag den 19. december 2019 kl. 10

Følg os på de sociale medier:

WEEK 11 OF THE COURSE

Expanding the Android Security Rewards Program

ANDROID SECURITY REWARDS (ASR) PROGRAM

- Created in 2015 to reward researchers who find and report security issues to help keep the Android ecosystem safe.
- Over the past 4 years: awarded over 1,800 reports
- Paid out > 4 million dollars.
- Last 12 months: 1.5 million dollars

TITAN M SECURE ELEMENT

Introduced within the Pixel 3 smartphones last year, Google’s Titan M secure element is a **dedicated security chip** that sits alongside the main processor, primarily designed to protect devices against the **boot-time attacks**.

TOP PRICE EXPANSION

Google just blogged

- Introducing a top prize of $1 million for a full chain remote code execution exploit with persistence which compromises the Titan M secure element on Pixel devices.
- Launching a specific program offering a 50% bonus for exploits found on specific developer preview versions of Android
  - Top prize is now $1.5 million.

TOP PAYOUT

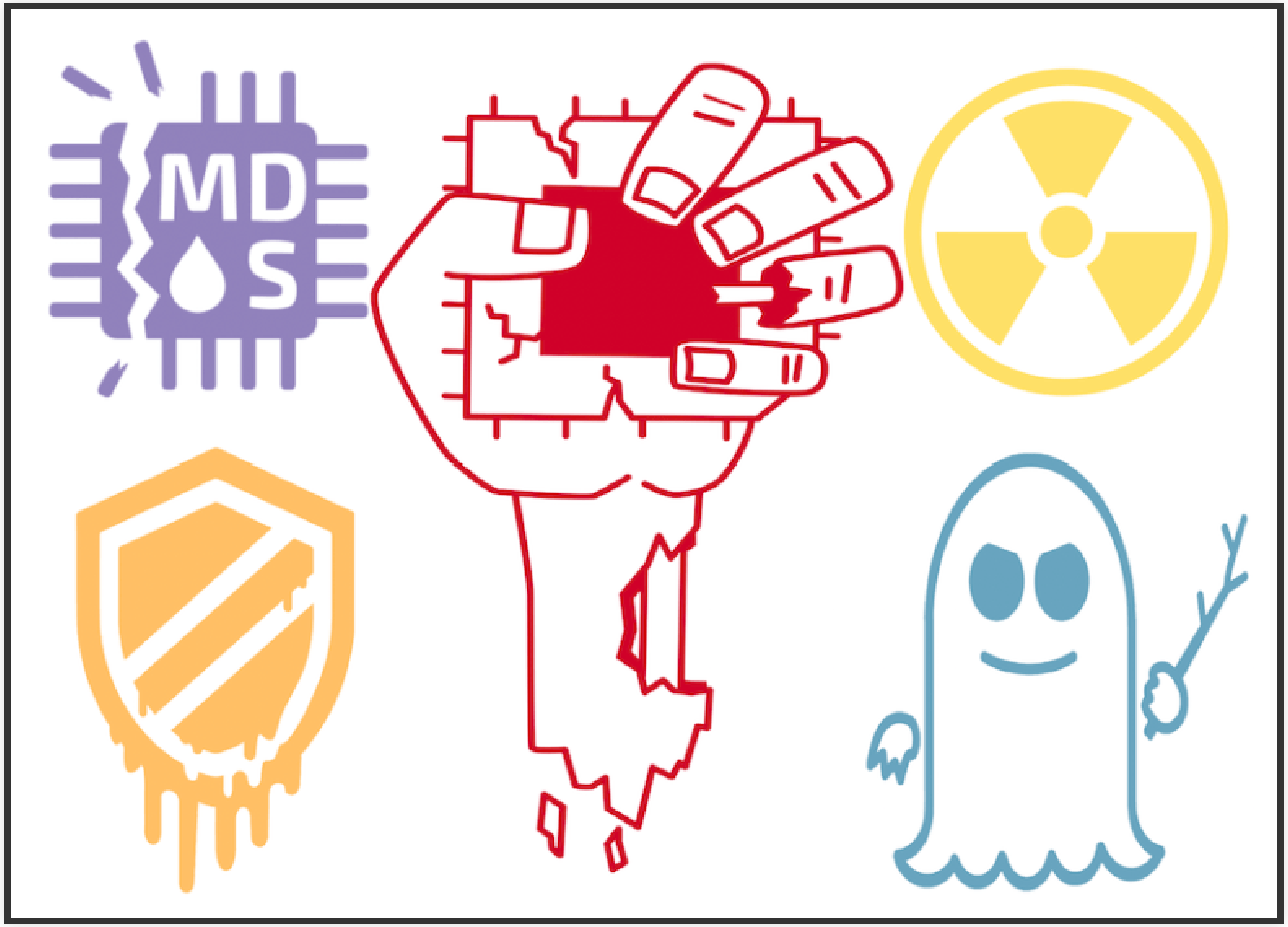
- **Guang Gong** of Alpha Lab, Qihoo 360 Technology Co. Ltd.
- First reported 1-click remote code execution exploit chain on the Pixel 3 device.
- Awarded $161,337 from the Android Security Rewards program and $40,000 by Chrome Rewards program for a total of **$201,337**.

COMMENTS

RESOURCES

- https://security.googleblog.com/2019/11/expanding-android-security-rewards.html
- Get started: https://sites.google.com/site/bughunteruniversity/improve/how-to-submit-an-android-platform-bug-report

WEEK 10 OF THE COURSE



ZOMBIELOAD V2

> We will take a look at a series of hardware based attacks - the latest published Nov. 14th.

Separate slides have the full info.

- https://thehackernews.com/2019/11/zombieload-cpu-vulnerability.html (v2)

WEEK 9 OF THE COURSE

Could have taken:

- Chinese Hackers Compromise Telecom Servers to Spy on SMS Messages
- Targeted Ransomware Attacks in Spain
- Chrome 0-day bugs under active attack
- Two Unpatched Critical RCE Flaws Disclosed in rConfig

Took the next

BLUEKEEP RDP FLAW SPOTTED IN THE WILD

https://thehackernews.com/2019/11/bluekeep-rdp-vulnerability.html

BACKGROUND

MORE BACKGROUND

- Many security firms and individual cybersecurity researchers who successfully developed a fully working exploit for BlueKeep pledged not to release it to the public
- Nearly 1 million systems were found vulnerable even a month after patches were released.

ISSUE

Amateur hackers took almost six months to come up with a BlueKeep exploit that is still unreliable and doesn’t even have a wormable component.

But now Bluekeep exploit in the wild

ANALYSIS

- Kevin Beaumont - had multiple EternalPot RDP **honeypot** systems got crashed and rebooted suddenly.
- Marcus Hutchins (the researcher who helped stop the WannaCry ransomware outbreak in 2017) analysed the crash dumps shared by Beaumont and confirmed **"BlueKeep artifacts in memory and shellcode to drop a Monero Miner."**

EXPLOIT DETAILS

The exploit contains encoded PowerShell commands as the initial payload, which then eventually downloads the final malicious executable binary from a remote attacker-controlled server and executes it on the targeted systems.

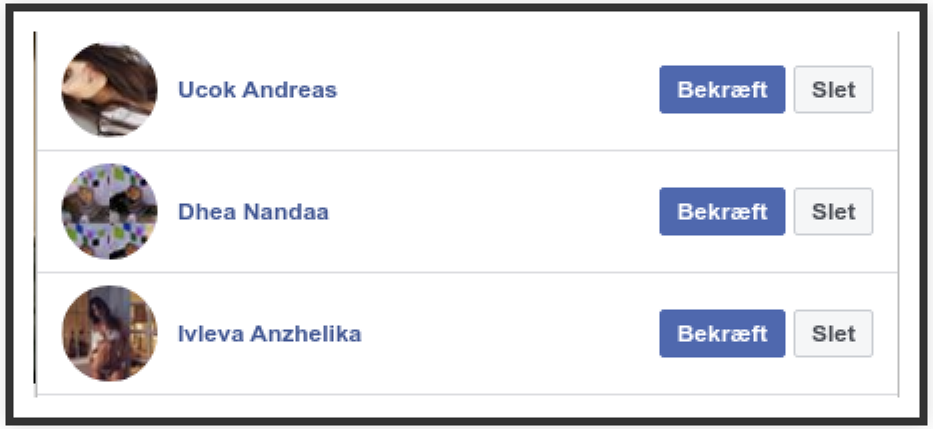
FIX

- Patch systems
- Disable RDP services, if not required.
- Block port 3389 using a firewall or make it accessible only over a private VPN.
- Enable Network Level Authentication (NLA) – this is partial mitigation to prevent any unauthenticated attacker from exploiting this Wormable flaw.

COMMENTS

WEEK 8 OF THE COURSE

PROFILE COPYING/IDENTITY THEFT



Ucok Andreas

Dhea Nandaa

Ivleva Anzhelika

THE CASE (1)

- My girlfriend - friday afternoon
- Several FB friends wrote to her about "another profile with the same name and pictures" asking for friendship
- Some accepted
- Soon they received a messenger message: "Can I have your phone number, please"
- Some replied "How come?" or "Sure, why?"
    - End of that communication

THE CASE (2)

- A few sent them their number
- Next message received was: "If you receive an SMS text, please pass it on to me, it is part of a competition."
- At least one replied with the SMS text
    - End of that communication

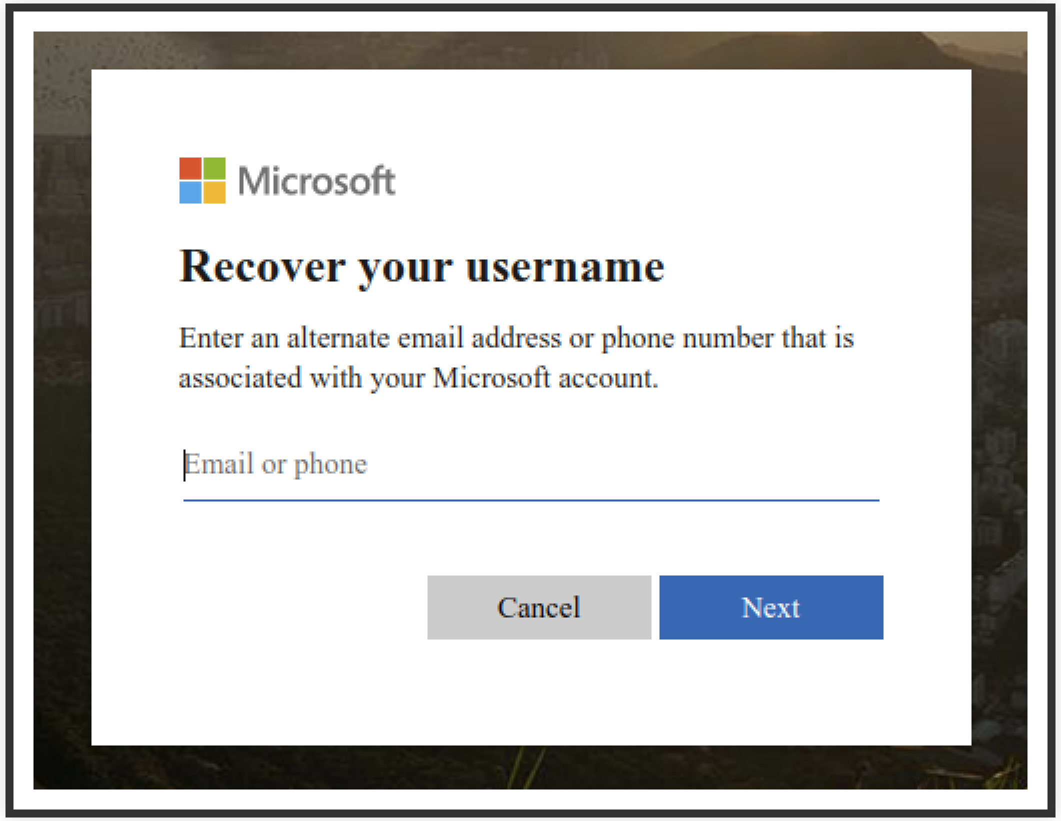
NEXT PART

- One friend next lost access to Instagram profile
- And mail account
- And... ???

WHAT HAPPENED?

- When you are friends - you can see each others mail addresses.

WHAT HAPPENED?



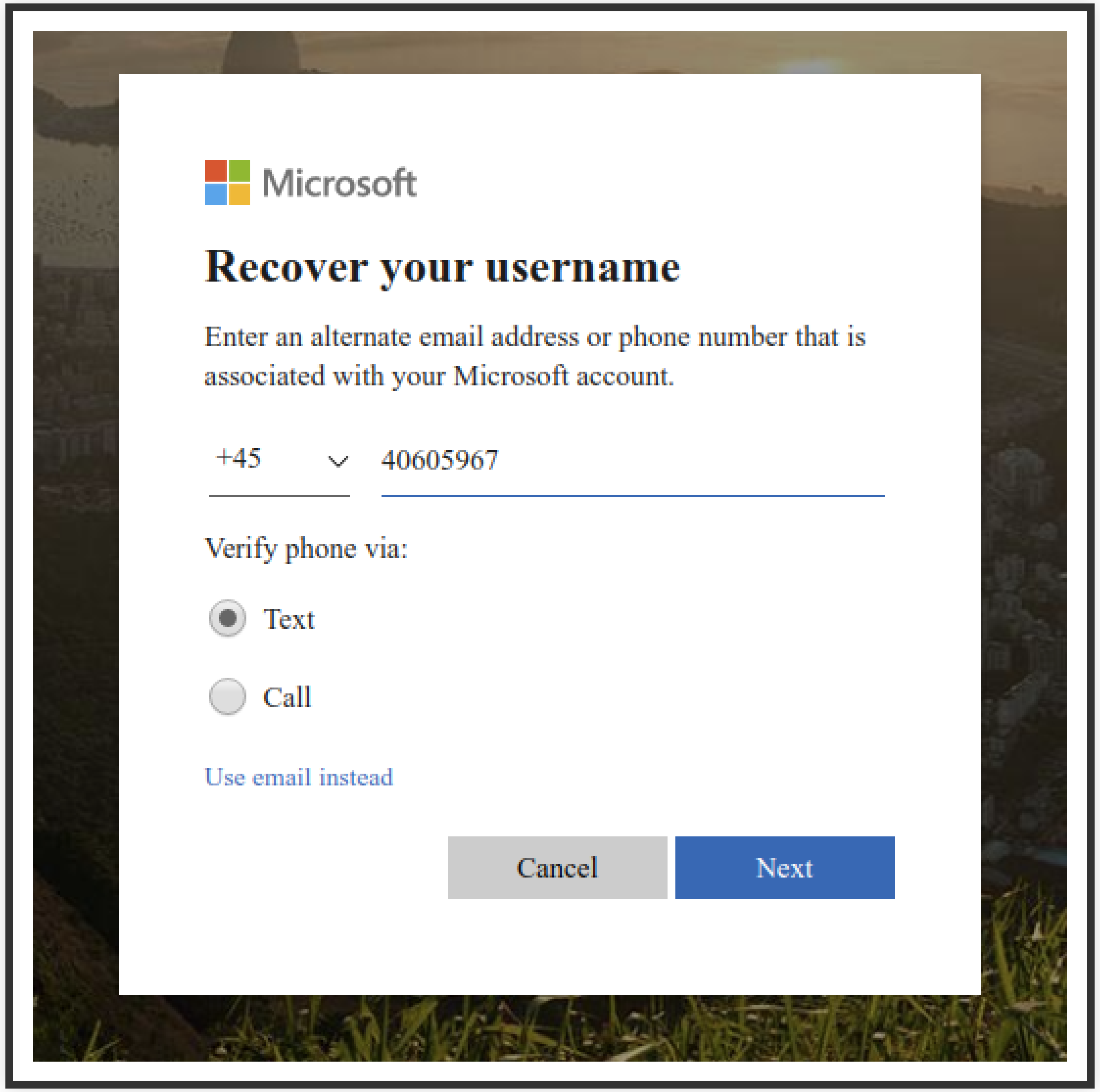
Microsoft

Recover your username

Enter an alternate email address or phone number that is associated with your Microsoft account.

Email or phone

WHAT HAPPENED?



Microsoft

Recover your username

Enter an alternate email address or phone number that is associated with your Microsoft account.

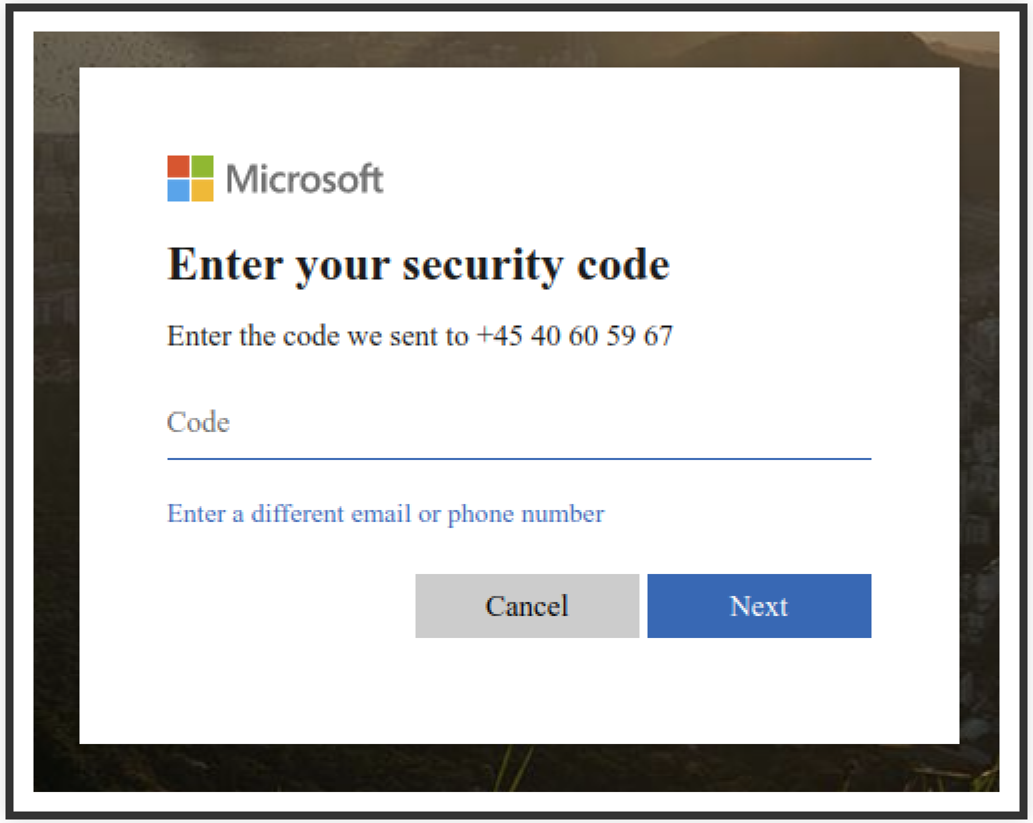
+45 40605967

Verify phone via:

● Text

○ Call

WHAT HAPPENED?



Microsoft

Enter your security code

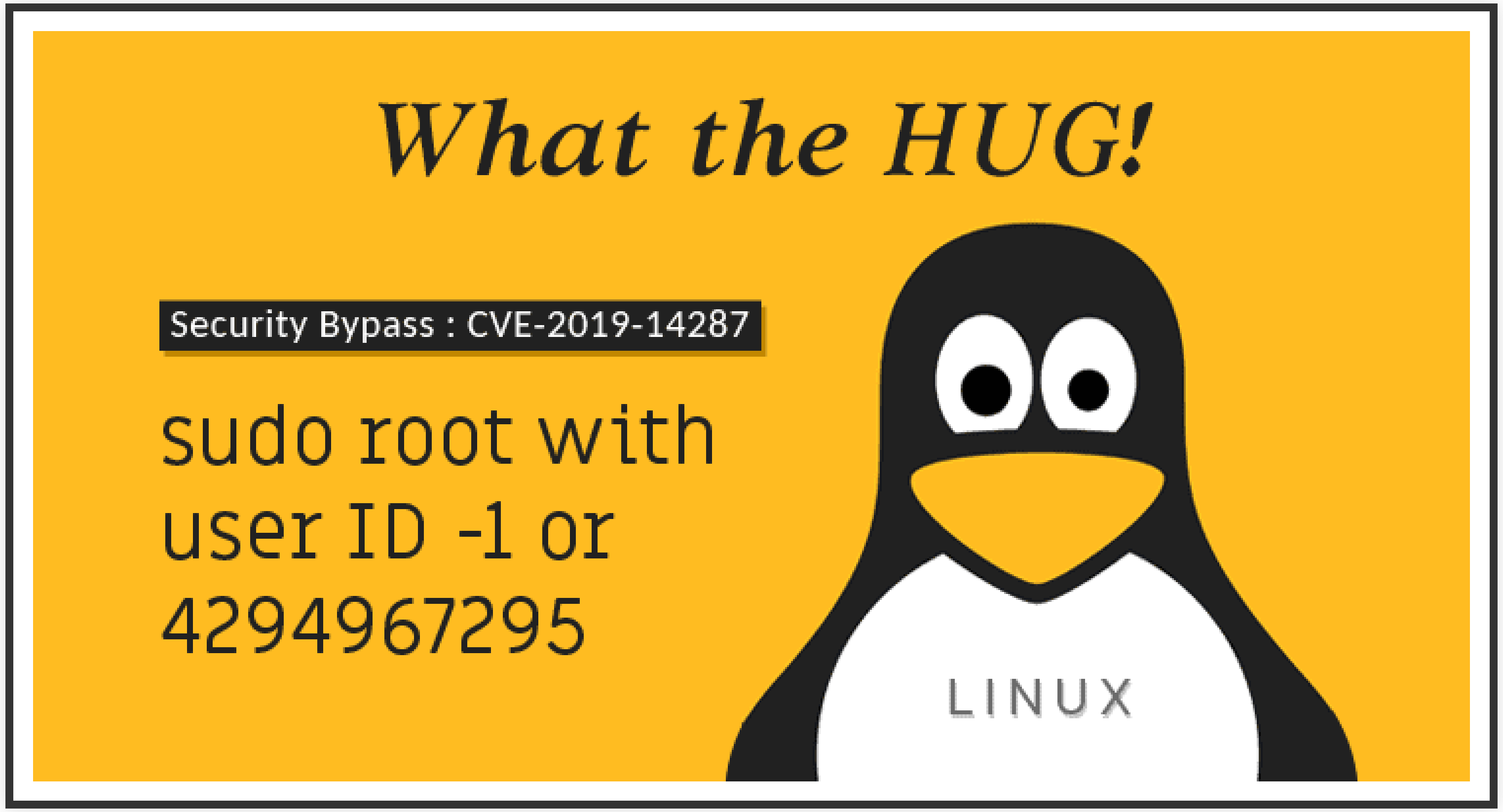
Enter the code we sent to +45 40 60 59 67

WHAT HAPPENED?

- When you have access to mail → lots of different signup letters and "Reset password" methods are available.
- What about the Instagram account → smokescreen
  - Keeps the friend occupied and unfocussed → Longer time to access other accounts.

COMMENTS AND DISCUSSION

WEEK 7 OF THE COURSE



What the HUG!

Security Bypass : CVE-2019-14287

sudo root with user ID -1 or 4294967295

ISSUE IN SHORT

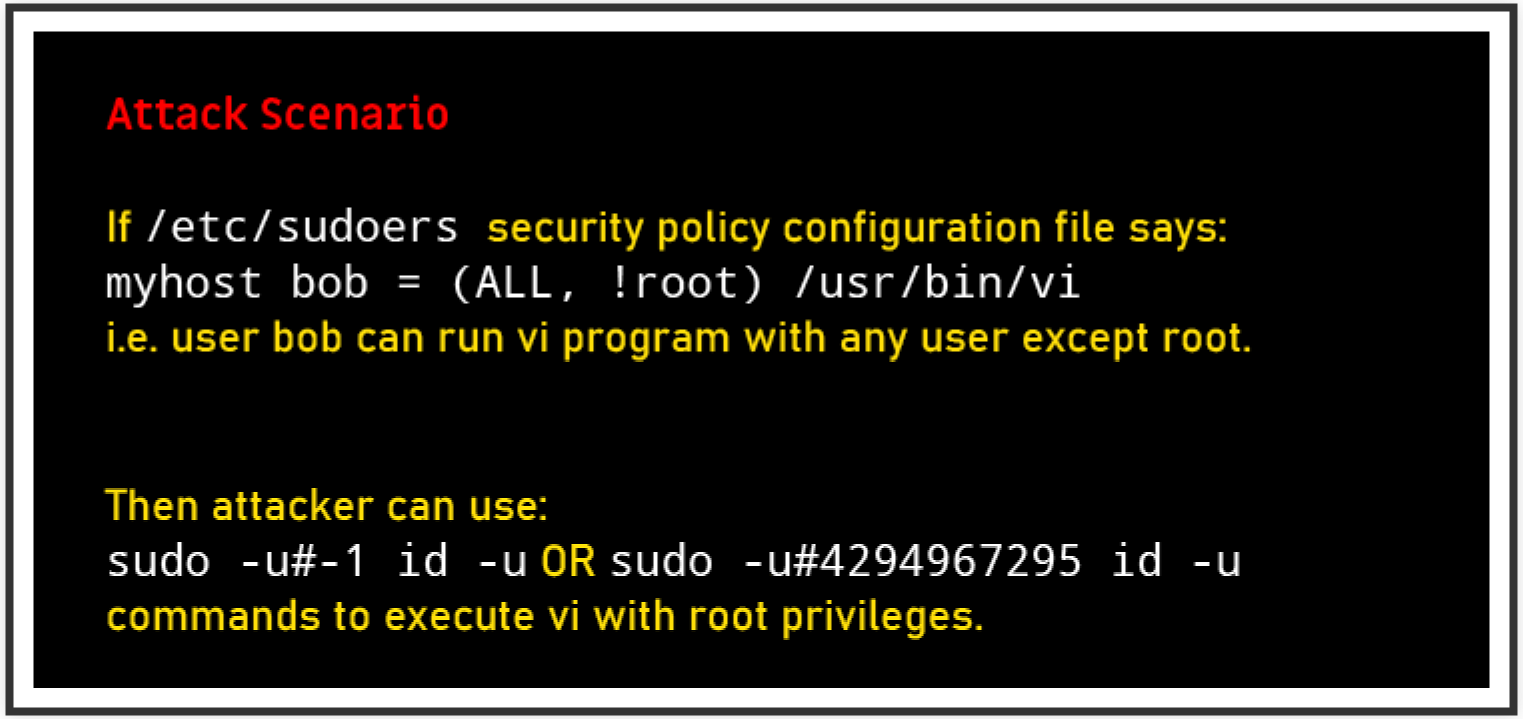
- Vulnerability in `sudo`
- CVE-2019-14287
- Discovered by Joe Vennix of Apple Information Security
- Privilege separation is one of the fundamental security paradigms in Linux, administrators can configure a sudoers file to define which users can run what commands as to which users.
- Affects all Sudo versions prior to the latest released version 1.8.28, which has been released

ISSUE IN SHORT

> *This can be used by a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access as long as the ALL keyword is listed first in the Runas specification*

— the Sudo developers.

ATTACK SCENARIO



Attack Scenario

If `/etc/sudoers` security policy configuration file says:

```
myhost bob = (ALL, !root) /usr/bin/vi
```

i.e. user bob can run vi program with any user except root.

Then attacker can use:

`sudo -u#-1 id -u` OR `sudo -u#4294967295 id -u`

commands to execute vi with root privileges.

COMMENTS AND DISCUSSION

RESOURCES

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287
- https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html

WEEK 6 OF THE COURSE

What if an innocent-looking GIF greeting with Good morning, Happy Birthday, or Merry Christmas message hacks your smartphone?

JUST A GIF IMAGE COULD HAVE HACKED YOUR ANDROID PHONE USING WHATSAPP

- Discovered by Vietnamese security researcher Pham Hong Nhat in May
- CVE-2019-11932 - a double-free memory corruption bug
  - Not actually reside in the WhatsApp code itself, but in an open-source GIF image parsing library that WhatsApp uses.
- Remote code execution attacks, enabling attackers to execute arbitrary code on targeted devices in the context of WhatsApp with the permissions the app has on the device.

ISSUE IN SHORT

> *Malicious code will have all the permissions that WhatsApp has, including recording audio, accessing the camera, accessing the file system, as well as WhatsApp's sandbox storage that includes protected chat database and so on...*

— The Hacker News

ISSUE IN SHORT

- The issue affects WhatsApp versions 2.19.230 and older versions running on Android 8.1 and 9.0, but does not work for Android 8.0 and below.
- reported the vulnerability to Facebook, who owns WhatsApp, in late July this year, and the company included a security patch in WhatsApp version 2.19.244, released in September.
- The developer of the affected GIF library, called Android GIF Drawable, has also released version 1.2.18 of the software to patch the double-free vulnerability.

COMMENTS AND DISCUSSION

RESOURCES

- https://thehackernews.com/2019/10/whatsapp-rce-vulnerability.html
- https://youtu.be/loCq8OTZEGI

WEEK 5 OF THE COURSE

ISSUE IN SHORT

- DoorDash: a popular on-demand food-delivery service
- Breach Exposes 4.9 Million Users' Personal Data
- Dates back 4 months! 4th May 2019
- The incident involves a third-party service provider.

DATA LEAKED

- Profile information of all 4.9 million affected users
  - Names, email addresses, delivery addresses, order history, phone numbers, and hashed passwords.
- Financial information of some consumers (last 4 digits of credit cards)
- Financial information of some Dashers and merchants (last 4 digits of credit cards)
- Information of 100,000 Dashers - driver’s license numbers

COMMENTS AND DISCUSSION

RESOURCES

- https://blog.doordash.com/important-security-notice-about-your-doordash-account-ddd90ddf5996
- https://thehackernews.com/2019/09/doordash-data-breach.html

WEEK 4 OF THE COURSE

https://thehackernews.com/2019/09/phpmyadmin-csrf-exploit.html

ISSUE IN SHORT

- Unpatched zero-day vulnerability in phpMyAdmin revealed
- Discovered by security researcher Manuel Garcia Cardenas
- Cross-site request forgery (CSRF) flaw, wherein attackers trick authenticated users into executing an unwanted action.
- CVE-2019-12922: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12922
- Deleting any server in the Setup page.
  - Cannot delete tables/data

ISSUE IN SHORT

> *The attacker can easily create a fake hyperlink containing the request that wants to execute on behalf of the user, in this way making possible a CSRF attack due to the wrong use of HTTP method," Cardenas explains in a post to the Full Disclosure mailing list.*

— Wang Wei on The Hacker News

EXPLOIT CSRF - DELETING MAIN SERVER

```
<p>Deleting Server 1</p>
<img src="
http://server/phpmyadmin/setup/index.php?page=servers&mode=remove&id=1"
style="display:none;" />
```

COMMENTS AND DISCUSSION

- What is CVE
- What is a zero-day vulnerability
- Ethics and best practices for announcing vulnerabilities

BONUS

- Cardenas discovered this vulnerability back in June 2019
- responsibly reported it to the project maintainers
- phpMyAdmin maintainers failed to patch the vulnerability within 90 days of being notified
- release the vulnerability details and PoC to the public on 13 September

WEEK 3 OF THE COURSE

FIREFOX AND DOH DNS

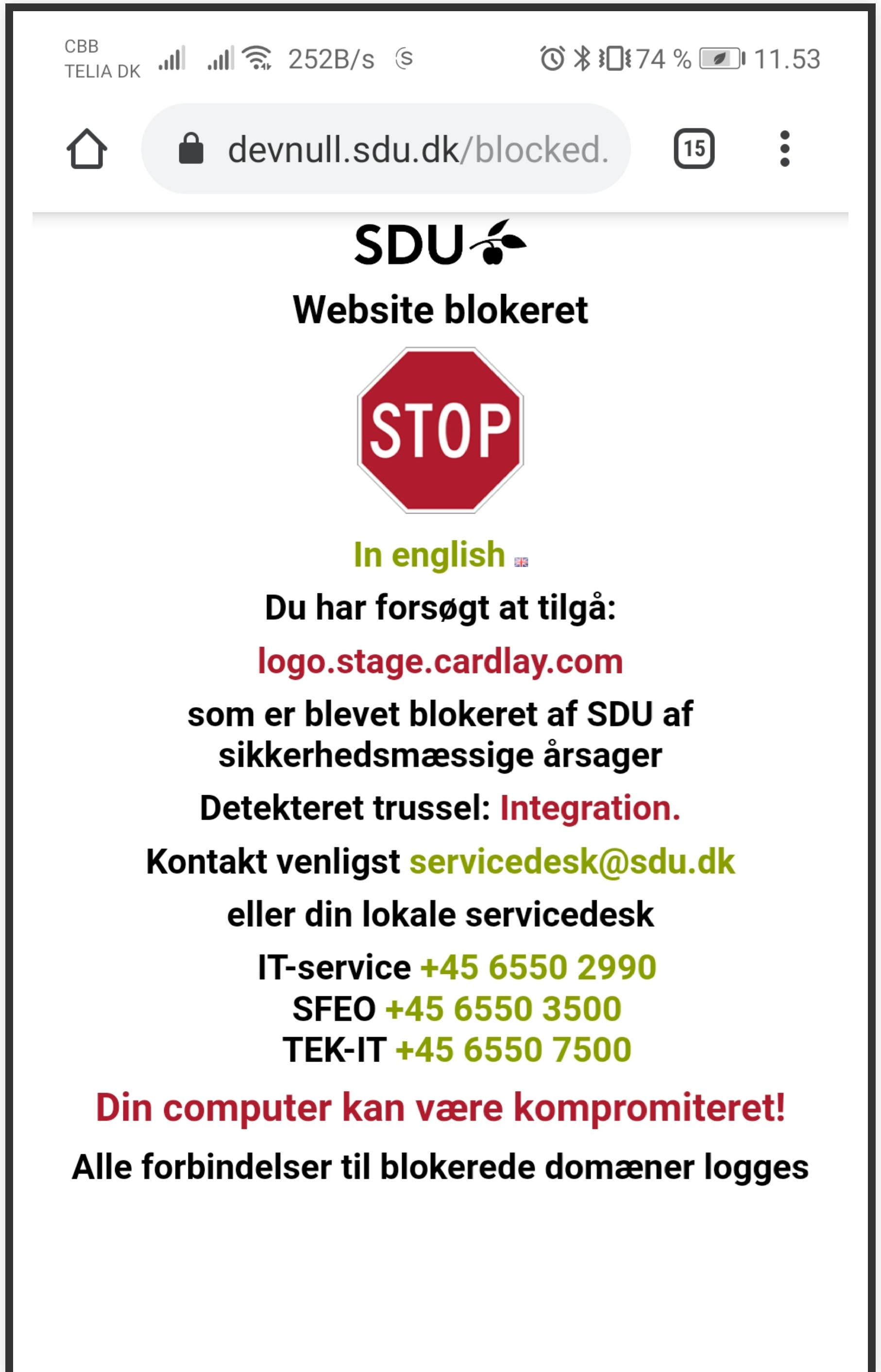
https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

ISSUE IN SHORT

The DoH protocol (DNS over HTTPS) was designed to enhance overall security of Internet users by sending DNS queries and getting DNS responses over HTTP using TLS security, which improves both integrity and confidentiality.

- Default in the US at first, but planned for all over the world next

WHAT DOES NOT HAPPEN (1)



Website blokeret

In english

Du har forsøgt at tilgå:

logo.stage.cardlay.com

som er blevet blokeret af SDU af sikkerhedsmæssige årsager

Detekteret trussel: Integration.

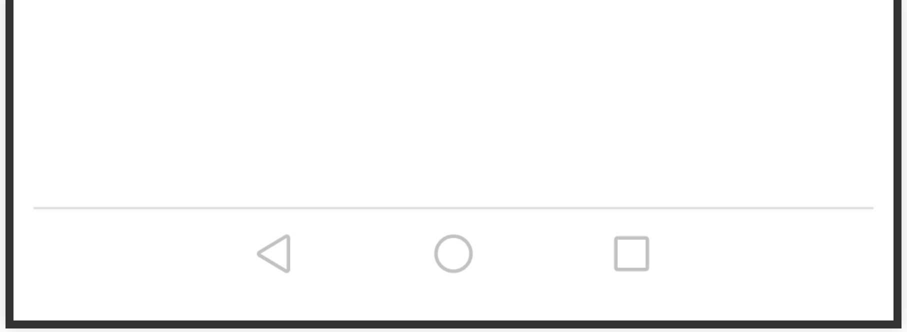
Kontakt venligst servicedesk@sdu.dk

eller din lokale servicedesk

IT-service +45 6550 2990
SFEO +45 6550 3500
TEK-IT +45 6550 7500

Din computer kan være kompromiteret!

Alle forbindelser til blokerede domæner logges



WHAT DOES NOT HAPPEN (2)

Imagine child pornography image here!

ISSUE IN SHORT

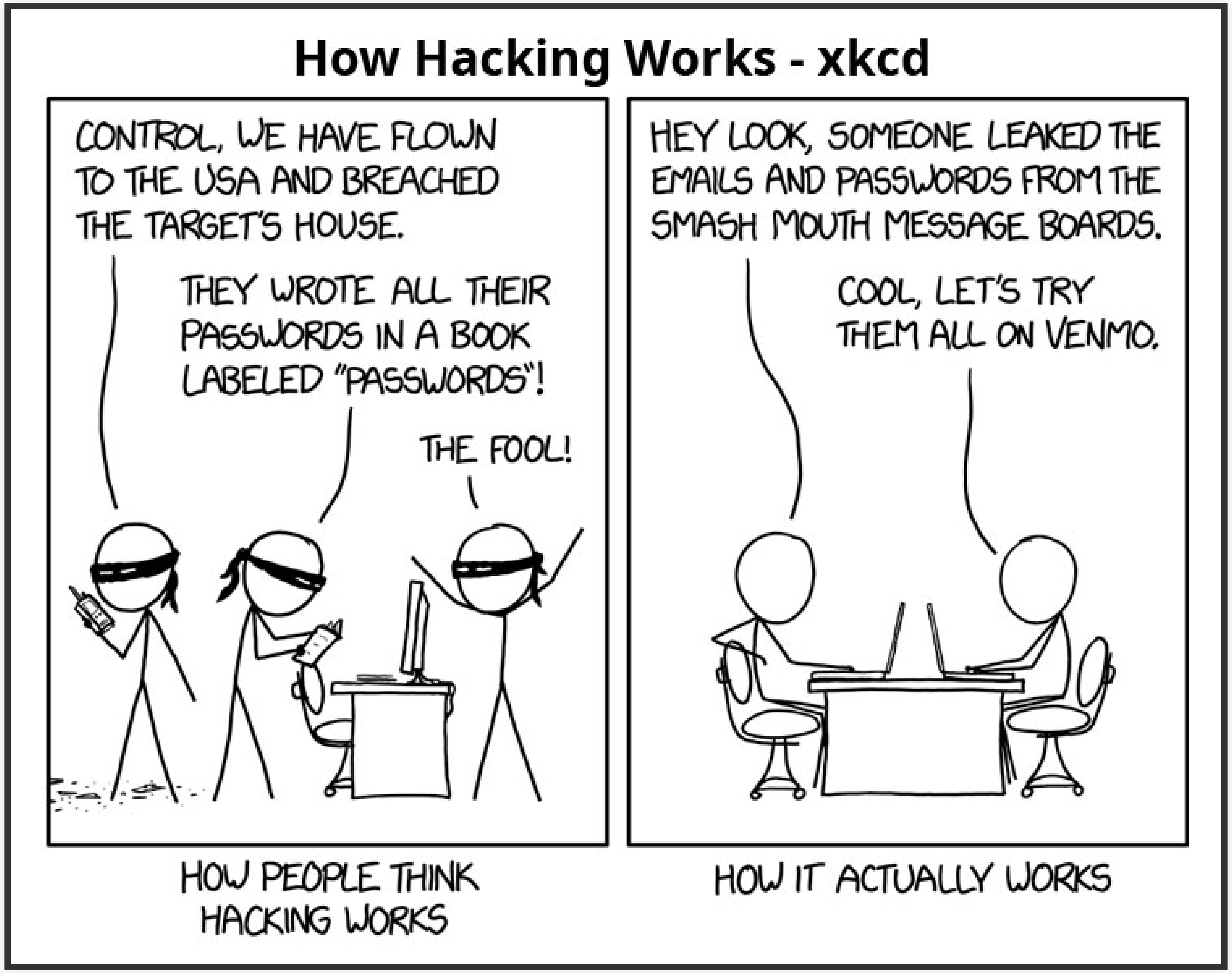
- Cannot intercept and monitor DNS queries
- Cannot make DNS blocking
- Planned togeather with Cloudflare
- Bypassing locally held DNS nameservers
- Many of the filtering and protection tools in place today, usually administered by ISPs, will no longer work.

COMMENTS AND DISCUSSION

RESOURCES

WEEK 2 OF THE COURSE

XKCD FORUM HACKED


How Hacking Works - xkcd
CONTROL, WE HAVE FLOWN TO THE USA AND BREACHED THE TARGET'S HOUSE.
THEY WROTE ALL THEIR PASSWORDS IN A BOOK LABELED "PASSWORDS"!
THE FOOL!
HOW PEOPLE THINK HACKING WORKS
HEY LOOK, SOMEONE LEAKED THE EMAILS AND PASSWORDS FROM THE SMASH MOUTH MESSAGE BOARDS.
COOL, LET'S TRY THEM ALL ON VENMO.
HOW IT ACTUALLY WORKS

ISSUE IN SHORT

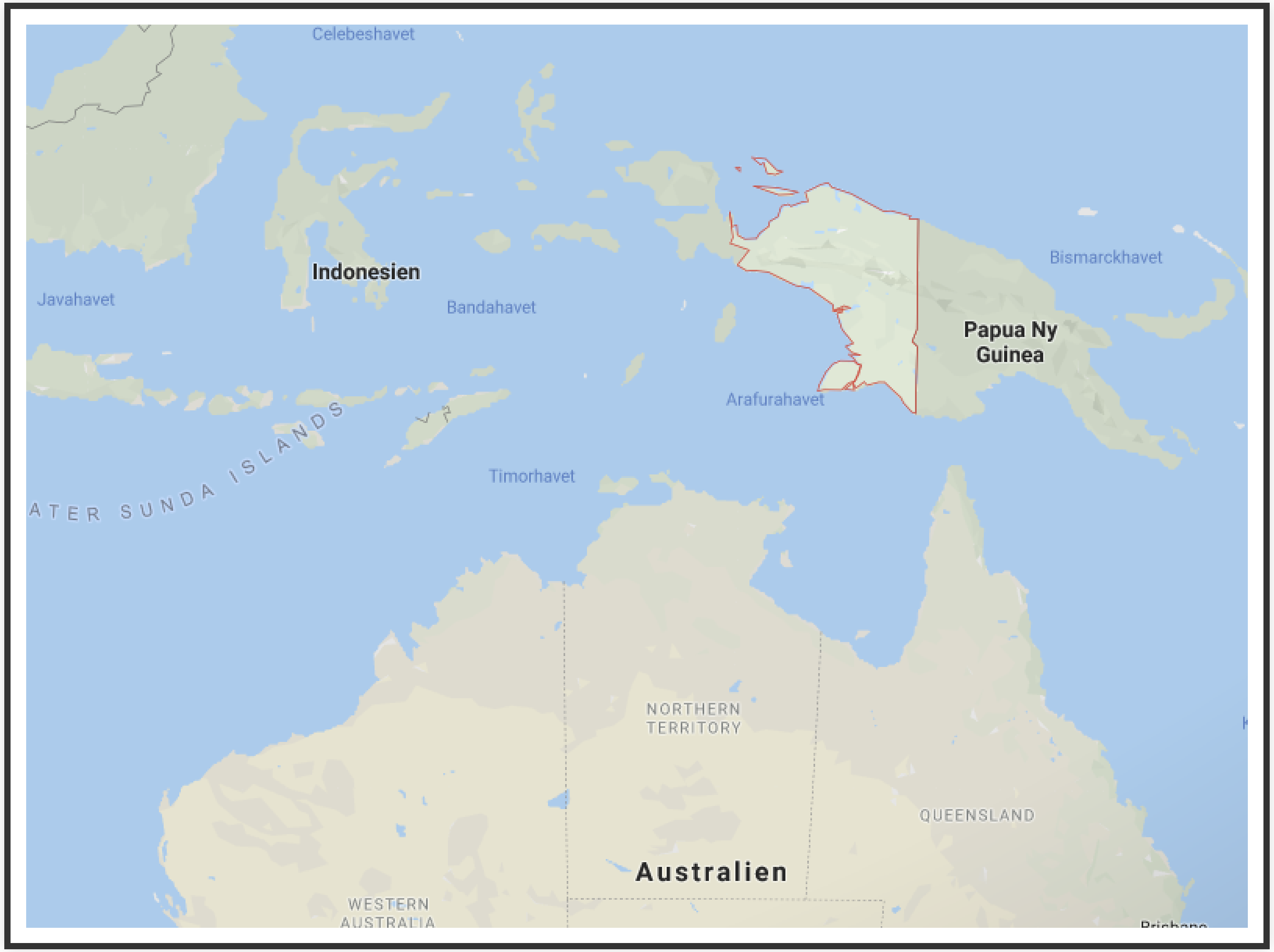
- Unknown hackers stealing around 562,000 usernames, email and IP addresses, as well as hashed passwords.
- XKCD uses phpBB, a free and open-source forum and bulletin board software built in the PHP programming software.
- BCRYPT hashing algorithm/ for early users: MD5 hashing method.

COMMENTS

RESOURCES

- https://thehackernews.com/2019/09/xkcd-forum-hacked.html
- https://forums.xkcd.com

WEEK 1 OF THE COURSE



ISSUE IN SHORT

The Indonesian government has blocked internet access as they deployed security forces to its easternmost provinces following days of violent protests there.

Second time in 2019 the Indonesian government blocked internet access as a response to political events.

COMMENTS

RESOURCES

- http://theconversation.com/the-internet-shutdown-in-papua-threatens-indonesias-democracy-and-its-peoples-right-to-free-speech-122333
- https://www.bbc.com/news/av/world-asia-49442819/indonesia-cuts-off-internet-to-papua-following-protests

https://thehackernews.com/2019/09/xkcd-forum-hacked.html