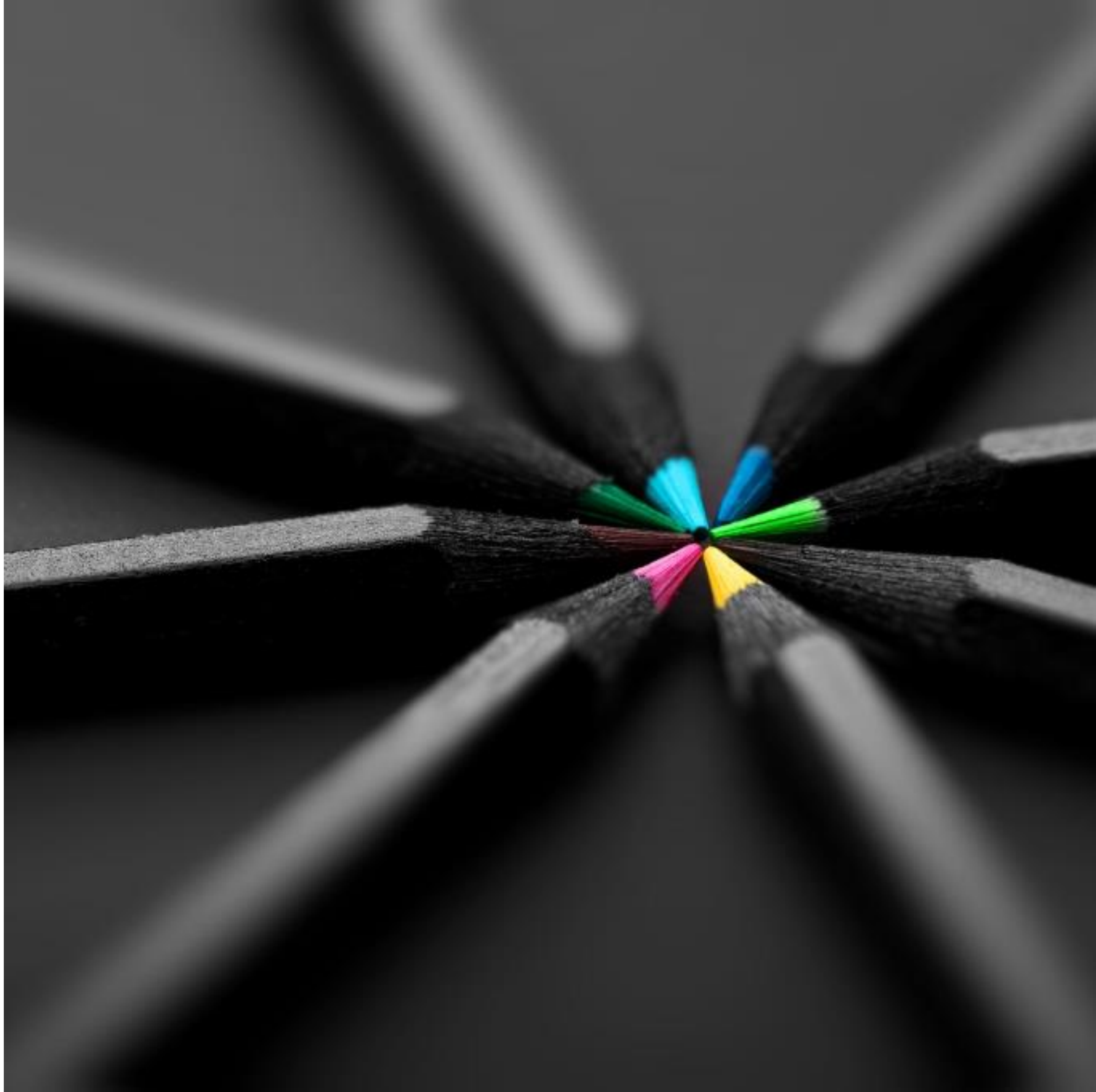
Allianz

Allianz Human Firewall

Red vs Blue Hat

Global



Your Speakers

Daria Catalui

Leading Allianz Group
Human Firewall since 2019

Daniela Gaipl

Customer Frontend Lead for
the Allianz CDC

Lars König

Allianz Global Lead for
Detection and Response

Allianz

enisa
European Network and Information Security Agency

Catch me – if you can!

A real vishing case

The Attack

Vishing is the short version of Voice Phishing

Attacker

Allianz Red Team member trying to gain access to the victim system

Victim

Allianz Employee

The Attack

What made this possible?

Reconnaissance

Find a victim & phone number

Identification of the victim and background data via openly accessible social media sites like linked in

Find a tool the victim is using

Using previous "benign" recon via the meta data in emails to identify internally used tools

Identify numbers used by support team

OSINT* search of leaked documents including support materials

Technology

Caller ID Spoofing of support number

Usage of caller ID spoofing to establish initial trust with the victim by displaying a trusted number.

Convincing Phishing Site

Creation of a convincing phishing page allowing the download of the malicious update.

*Open Source Intelligence

The Attack

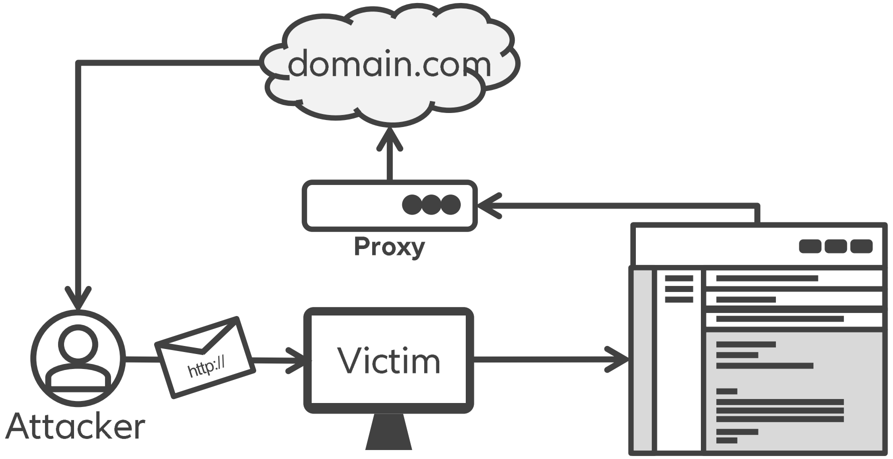
Find a tool the victim is using

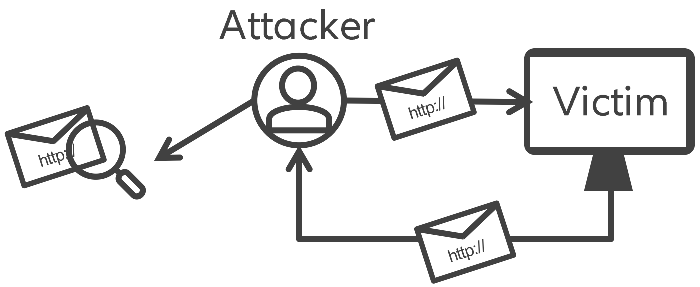
Network Tool

Usage of images/ links in mails to identify the proxy or browser used by the victim.

Email Tool

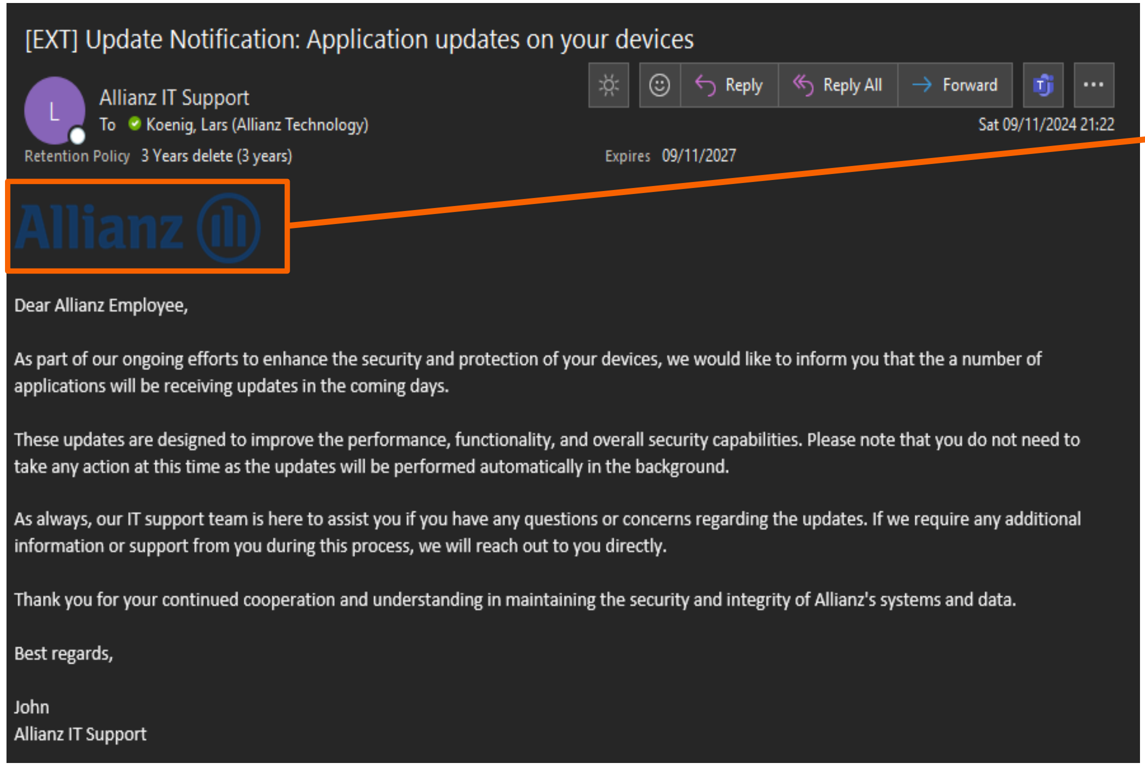
Usage of the meta data in response emails to identify internally used systems.





The Attack

Find a tool the victim is using



[EXT] Update Notification: Application updates on your devices

Allianz IT Support

To Koenig, Lars (Allianz Technology)

Sat 09/11/2024 21:22

Retention Policy 3 Years delete (3 years) Expires 09/11/2027

Dear Allianz Employee,

As part of our ongoing efforts to enhance the security and protection of your devices, we would like to inform you that the a number of applications will be receiving updates in the coming days.

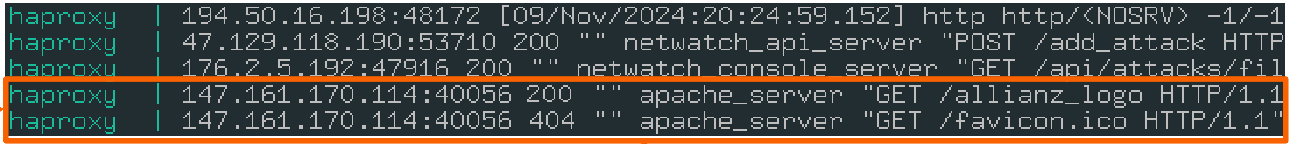
These updates are designed to improve the performance, functionality, and overall security capabilities. Please note that you do not need to take any action at this time as the updates will be performed automatically in the background.

As always, our IT support team is here to assist you if you have any questions or concerns regarding the updates. If we require any additional information or support from you during this process, we will reach out to you directly.

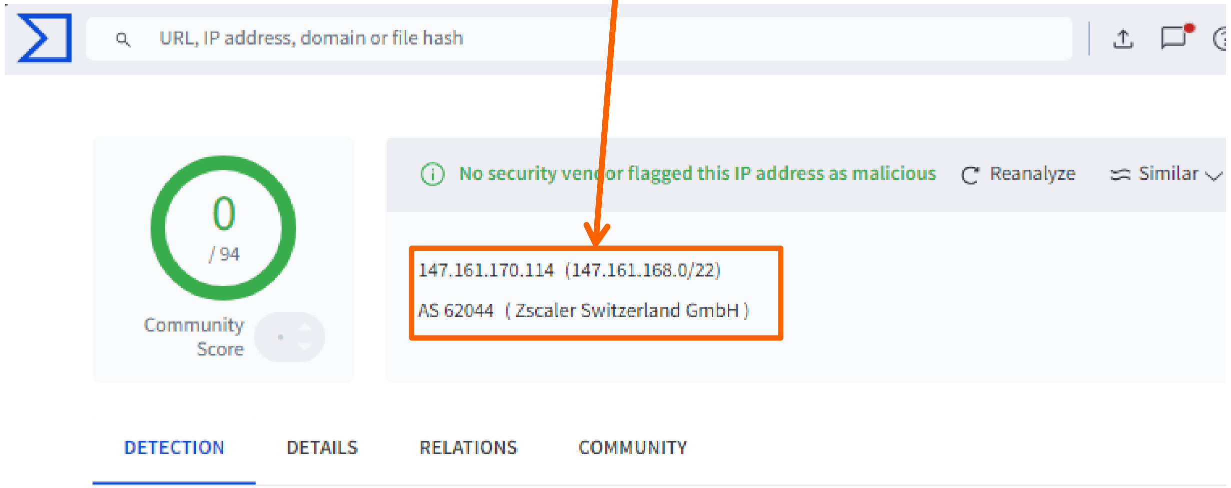
Thank you for your continued cooperation and understanding in maintaining the security and integrity of Allianz's systems and data.

Best regards,

John
Allianz IT Support



```
haproxy  | 194.50.16.198:48172 [09/Nov/2024:20:24:59.152] http http/<NOSRV> -1/-1
haproxy  | 47.129.118.190:53710 200 "" netwatch_api_server "POST /add_attack HTTP
haproxy  | 176.2.5.192:47916 200 "" netwatch_console_server "GET /api/attacks/fil
haproxy  | 147.161.170.114:40056 200 "" apache_server "GET /allianz_logo HTTP/1.1
haproxy  | 147.161.170.114:40056 404 "" apache_server "GET /favicon.ico HTTP/1.1"
```



No security vendor flagged this IP address as malicious

147.161.170.114 (147.161.168.0/22)

AS 62044 (Zscaler Switzerland GmbH)

Human Firewall debrief: Red vs Blue Hat

Human Firewall debrief

1 Objective & Preparation

Allianz

As attacker my AIM is to collect sensitive information from the victim, such as passwords, or login credentials or directly get access to the victims' systems.

Phase I: As attacker, I conduct reconnaissance to gather information about my target.

This can include:

- Public social media profiles (LinkedIn, Facebook) or other publicly accessible data sources.
- Information on the victim's employer or organization (e.g., phishing attempts disguised as IT department communications within a company).
- Identifying the victim’s preferred communication channel (phone, email, etc.).

V S

1st step to protection is to be aware of **what information** I share and **where**.

- Which of it is publicly accessible?
- How much do I share about my day-to-day work?
- How quickly can a GenAI application provide information about me?

2nd step is to get to know and understand the threat landscape and what are the tools that protect me. Enable them!

Human Firewall debrief

2 Attack techniques

Phase 2 is fun for me.

Building **trust** and **manipulation** (using information about victim)

- Create **urgency** (something that needs immediate resolution)
- Psychological **manipulation** (exploitation of fear, putting victim in stressful situations)
- **Technical tactics** (caller ID spoofing, fake website or login pages)

VS

Phase 2 is difficult for me.

Preventive security measures

- **Training & awareness**
  - Initial signs of phishing: check for discrepancies during the call, such as unusual language, strange requests, or questions asking for personal/confidential information.
  - Verification of information.
  - Reporting the incident.
- **Technological protection**
  - Spam & fraud filters (active blocking)
  - Caller ID verification
  - 2FA or MFA (to secure accounts and systems)

Human Firewall debrief

3 Success of the attack

Successful Execution is what I strive for.

- The victim unwittingly provides sensitive information, such as PINs, passwords, or personal details or as attacker I get access to the company's system.
- As attacker I can then use this information for malicious activities, such as transferring funds from the victim’s account or committing identity theft or access systems to steal sensitive information.

VS

Be resilient means getting thorugh it too. Know what can support me and stay focused to get back.

Immediate Action:

- If sensitive data has already been provided, an investigation is launched promptly.
- Passwords and accounts are locked or reset.
- A legal investigation may be initiated to track down the phishing attacker.
- Sharing the current campaign with the security community to foster awareness within the company.

Long-Term Measures:

- A thorough analysis is performed to understand how the attack occurred and which vulnerabilities were exploited.
- Additional training sessions and tests (e.g., phishing simulations) are conducted to strengthen awareness and detection of phishing attempts.

Next level

AI driven social engineering attacks

More Voice Cloning & Deepfakes are seen in the wild.

For an efficient attack, a threat actor might not just try to trick you with a **known voice** but maybe also with a **known face**.

Human Firewall always complements the Technical Firewall

Take the time to go through:

Analysis & Prevention

Why was the attack successful or not?

How to stop the next attack?

Connect to your peers to get inspired and enjoy your job

Allianz

enisa
European Network
and Information
Security Agency

About me

Daria Catalui, leading Allianz Group Human Firewall since 2019

AI generated avatar, real me?

- a cyber security professional always searching for impact and connecting ideas.
- over 15 years of experience at local, regional, and European level while working for EU’s cyber security agency ENISA, the European Commission and the RO Presidency of the Council of the EU.
- academic global initiative #CyberEDUcall4papers one of the few focusing on cyber education and the complementarity of a trained Human Firewall vs up to date Technical Firewall. Read more

Awards: 2024 OSPA Outstanding cyber security team GUA-Allianz Group

Women4Cyber 2020

Advisory: EU AI office Plenary member for Code of practice

ENISA advisory training and awareness, tireless ambassador :)

About me

Daniela Gaipl, Chapter Lead Product Owner in Information Security and Lead Customer Frontend in the Allianz Cyber Defense Center

- Over 7 years experience in the field of IT Operations and 4 years of experience in Information Security.
- Focusing on continuous development to break down silos and create synergies across departments.
- Leading customer-centric initiatives, ensuring transparency through reporting and clear communication, while enhancing the customer experience.

About me

Lars König
Allianz Global Lead for Detection and Response in
the in the Allianz Cyber Defense Center

'I look at the Human Firewall as essential to activate trained human sensors to support the Technical Firewall'