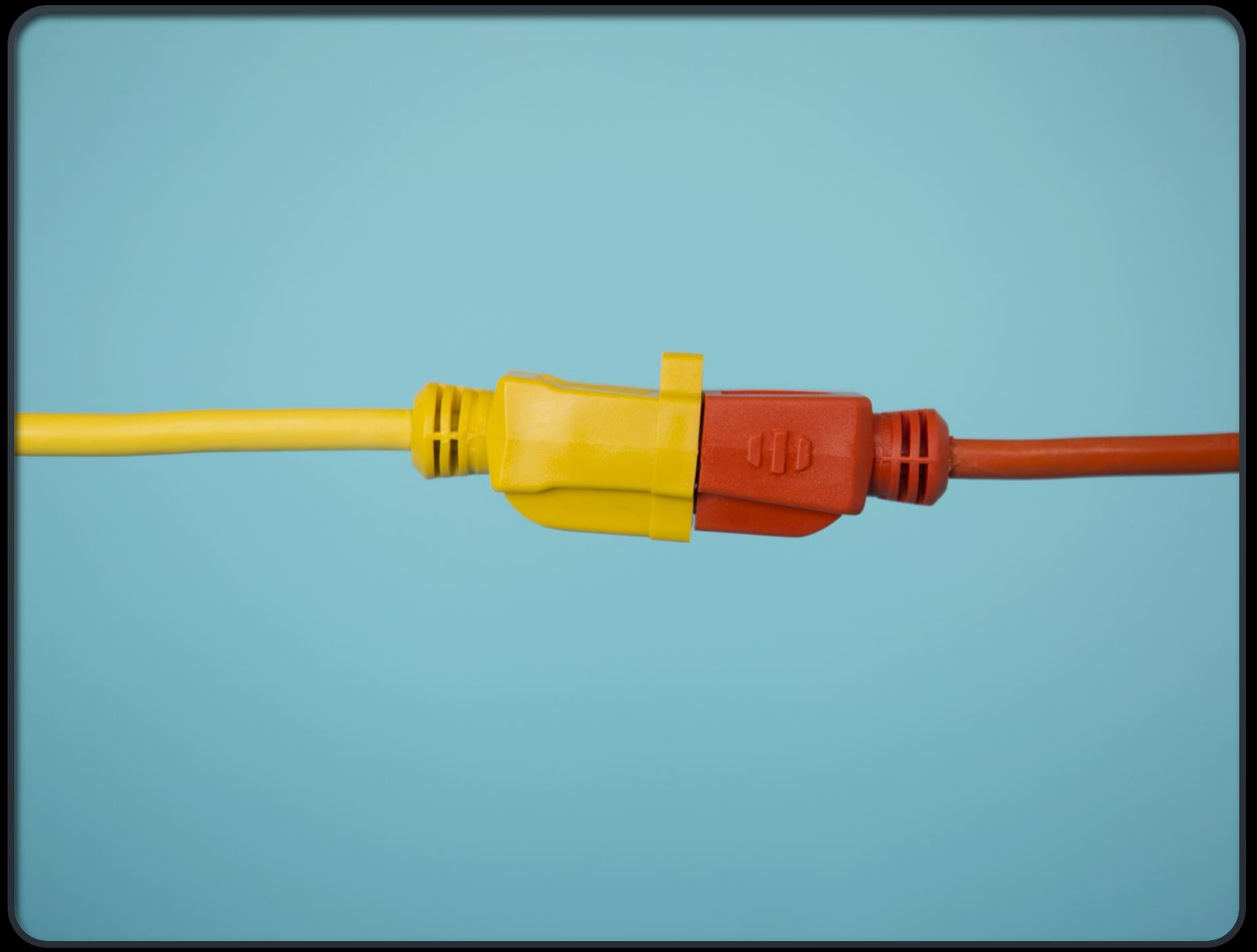
# PLUG & PRAY

Biztonsági rések a dobozból
frissen kicsomagolt modemeken

Matek Kamilló

2025.10.01



# WHOAMI?

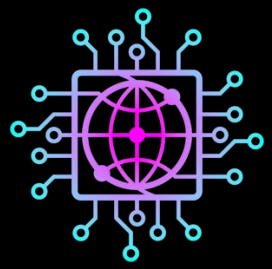
Matek Kamilló aka k4m1ll0

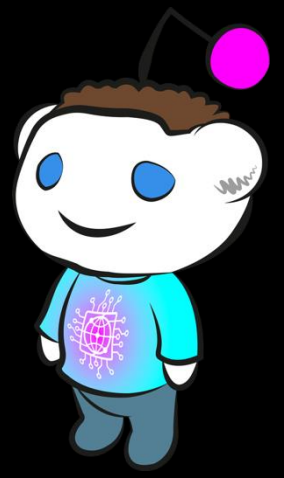
Ethical Hacker – Security Researcher

- Home page: https://k4m1ll0.com
- Public research: 15+ CVE, publikációk
  - https://www.bleepingcomputer.com/news/security/dark-mirai-botnet-targeting-rce-on-popular-tp-link-router/
  - Shift + F10 bypass – Microsoft https://k4m1ll0.com/ShiftF10Bypass-and-privesc.html
  - Red Teaming - Forcepoint https://k4m1ll0.com/forcepoint-dlp-redteam.html
  - TP-Link, Mercusys and other vulnerabilities
  - https://k4m1ll0.com/cve-2023-52162.html , and more …
- Cylantro Hacker közösség alapítója

GAMMAORG

Cylantro Labs Ltd.





# A HÁLÓZATI ESZKÖZ- ÉS BIZTONSÁGI TERMÉKGYÁRTÓK KÖRÜLI MÍTOSZ

- A különböző hálózati eszközgyártókat és biztonsági termékeket forgalmazó cégeket régóta körüllengi egyfajta mítosz. Ez a mítosz azt sugallja, hogy ha egy adott gyártó termékét választjuk, az automatikusan garantálja a teljes biztonságot, stabilitást és a problémamentes működést.
- Ez a hit azonban nem a valóságon alapszik. Sok esetben inkább a marketing gépezet terméke, mintsem a technikai valóságé.
- A mítoszt pedig nemcsak a gyártók tartják életben. Aktívan táplálják az online újságok, fizetett tartalmakon keresztül, a marketing anyagok túlzó állításai, sőt — **talán a legaggasztóbb** — néha maguk a **szakemberek** is. Olykor meggyőződésből, máskor egyszerű megszokásból továbbadják ezeket a tévhiteket.

Most csak a modemekről fogok beszélni …

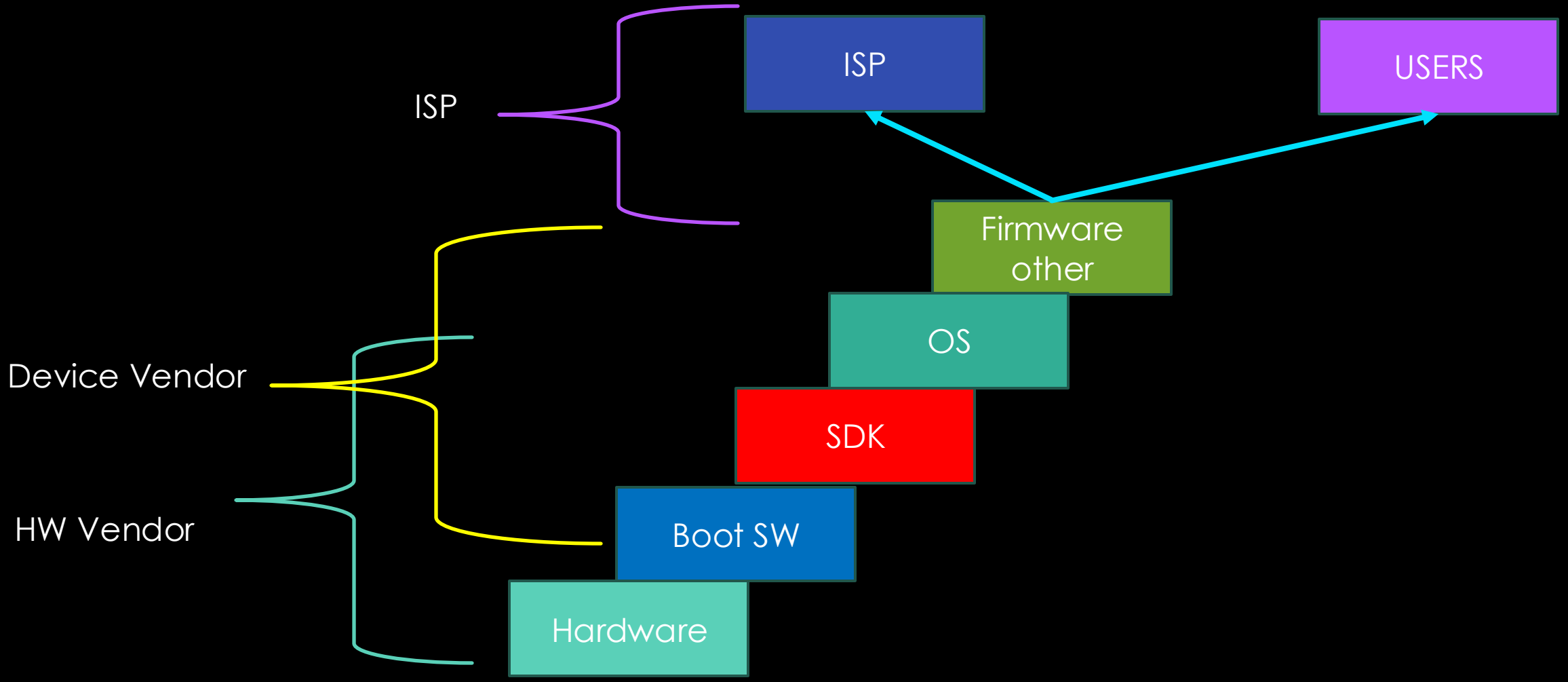
# MIÉRT ÉRDEMES A TÁMADÓKNAK A MODEMEKET ÉS HÁLÓZATI ESZKÖZÖKET CÉLBA VENNI?

- **GYENGE VÉDELEM**
  MODEMEK ÉS ROUTEREK GYAKRAN ÉVEKEN ÁT MŰKÖDNEK FRISSÍTÉS NÉLKÜL, GYÁRI JELSZAVAKKAL.
- **INTERNETKAPCSOLATI POZÍCIÓ**
  MINDEN ADAT RAJTUK KERESZTÜL HALAD – IDEÁLIS PONT MEGFIGYELÉSRE, ADATSZIVÁRGÁSRA, FORGALOM ÁTÍRÁSÁRA.
- **TÖMEGES JELENLÉT**
  UGYANAZ A TÍPUSÚ ESZKÖZ SOK TÍZEZER VAGY AKÁR MILLIÓ PÉLDÁNYBAN VAN KINT – HA EGYET FELTÖRNEK, MIND TÁMADHATÓ.
- **NEHÉZ ÉSZLELNI A TÁMADÁST**
  A LEGTÖBB FELHASZNÁLÓ NEM LÁTJA, MI TÖRTÉNIK A MODEMJÉN, ÉS A TÁMADÁS SOKÁIG ÉSZREVÉTLEN MARADHAT.
- **BELÉPÉSI PONT A BELSŐ HÁLÓZATBA**
  EGY SEBEZHETŐ MODEM VAGY GATEWAY HOZZÁFÉRÉST ADHAT AZ OTTHONI VAGY IRODAI HÁLÓZAT TÖBBI ESZKÖZÉHEZ.
- **BOTNETBE FOGHATÓ ERŐFORRÁS**
  FELTÖRT MODEMEK GYAKRAN VÁLNAK RÉSZÉVÉ BOTNETEKNEK (PL. MIRAI), DDOS-TÁMADÁSOKHOZ.

# KI FELEL VALÓJÁBAN A MODEMEK BIZTONSÁGÁÉRT? 1.

- A GYÁRTÓK
- A SZOLGÁLTATÓ
- A FELHASZNÁLÓK
- A SZOMSZÉD
- A SZERELŐ
- MINDENKI, SENKI?
- ÉN?

# MODEMEK, AHOGY ÉN LÁTOM

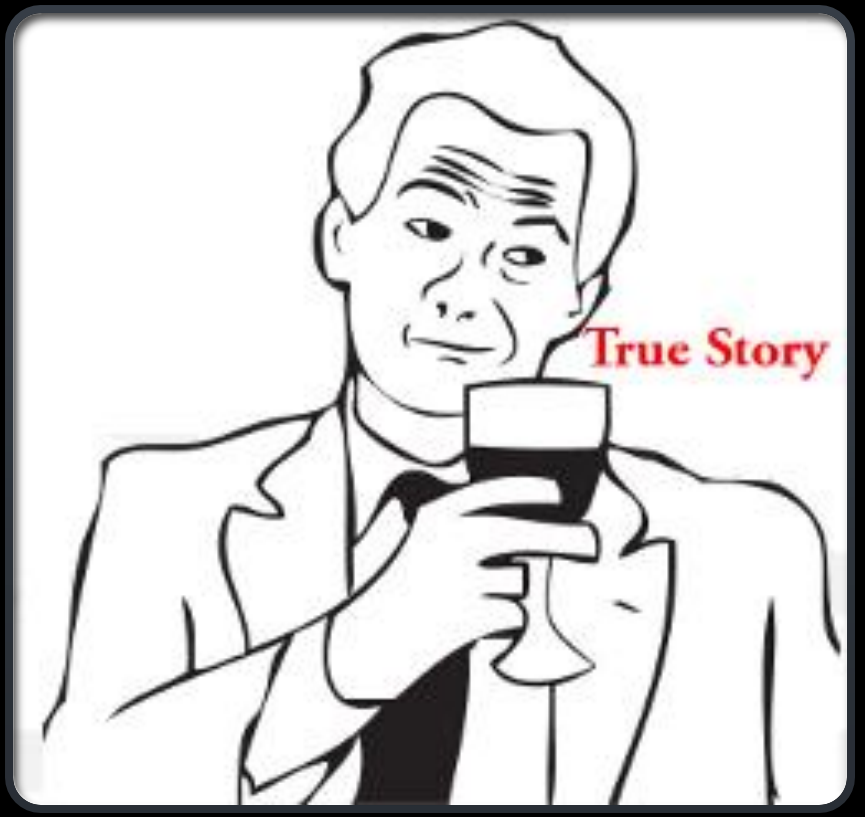


# KÜLÖNBÖZŐ SÉRÜLÉKENYSÉGEK AMIKRŐL JELENTÉST ÍRTAM

- Unauthenticated Access
- Buffer Overflow
- Misconfiguration
- Default Credentials
- Hardcoded Credentials
- Backdoor
- Outdated SDK
- Open Ports
- Remote Code Execution
- Command Injection
- Cross-Site Scripting (XSS)
- CSRF
- Information Disclosure
- Unauthenticated Access
- Weak Encryption
- Insecure Protocols
- Insecure Update Mechanism
- Privilege Escalation
- Telnet Enabled
- Debug Interface Enabled
- Insecure Cloud Integration (*)
- DNS Hijacking(*)
- Weak Password Policy
- Hidden Services
- Directory Traversal
- Missing Authentication
- UPNP Vulnerability
- SSH Vulnerabilities
- SSL Vulnerabilities
- Vulnerable Firmware checking
- Vulnerable Software Components
- SNMP
- …

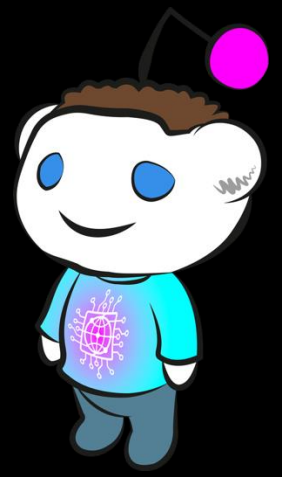
# STORY TIME

- Letiltott funkciók
- Buffer overflow
- UPNP
- Auth bypass
- SNMP



# TAKE AWAY

- A BIZTONSÁG NEM MARKETINGANYAGOKBAN DŐL EL. A TÉNYEKET ELLENŐRIZNI KELL – NEM ELHINNI.



# KÖSZÖNÖM A FIGYELMET!

KÉRDÉSEK?