Nation-Scale SecOps

How CERT PL Scans Poland

whoami

- Senior Threat Analysis Specialist, CERT PL
- Started as a software engineer
- Teaches offensive security at the University of Warsaw

Part 1: Artemis

Purpose of Artemis

After an incident, let's scan other entities for the same problem.

Motivation:

- Exposed code repository on an university website caused API key leak and unauthorized data access.
- Multiple BEC incidents caused by lack of DMARC.

A domain →  artemis →

1. The following addresses contain version control system data:

   - https://[redacted]:443/.git/

   (...)

A domain →  artemis →

1. The following addresses contain version control system data:

   - https://[redacted]:443/.git/

   (...)

2. The following addresses contain old Joomla versions:

   - https://[redacted]:443 - Joomla 2.5.4

   (...)

.gov.pl,
schools,
hospitals,
universities,
banks,
…

1. The following addresses contain version control system data:

   - https://[redacted]:443/.git/

   (...)

2. The following addresses contain old Joomla versions:

   - https://[redacted]:443 - Joomla 2.5.4

   (...)

What do we check?

A couple dozen modules

- Finding subdomains (e.g. cert.pl → test.cert.pl)
- Findings sites hosted on a given IP if scanning an IP range
- Domain expiration check
- Bad DNS configuration check:
  - Zone transfer
  - Subdomain takeover
- E-mail spoof protection mechanisms: SPF/DMARC
- Bad/expired TLS certificates, https:// redirect

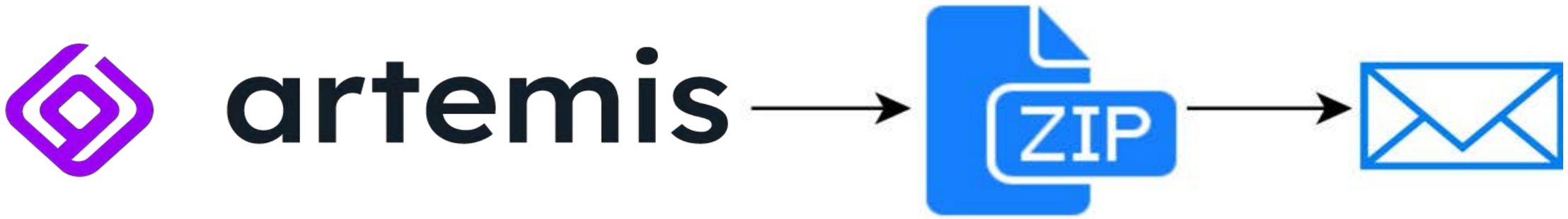
A couple dozen modules

- Port scanning, identifying services on a given server
- WordPress, WordPress plugin, Moodle, Drupal, Joomla, and Joomla extension version check
- Closed WordPress plugins
- **Nuclei support**: thousands of vulnerabilities and misconfigurations (from Open Redirects to RCEs)
- SQLi, XSS, RCE, SSRF, Local File Inclusion check (multiple tools, e.g. Nuclei or sqlmap)

A couple dozen modules

- Scripts loaded from nonexistent domains
- Directory index
- Weak passwords
- Exposed code repositories
- Exposed login panels, RDP ports, databases, …
- Accidentally published files (eg. /db.sql, /backup.zip or /wp-config.php.bak)
- **Possibility to integrate any other tool (commercial or open-source) + an example how to do that**

E-mail reports



Example e-mail

The following addresses contain version control system data:

- https://[redacted]:443/.git/

Making a code repository public may allow an attacker to learn the inner workings of a system, and if it contains passwords or API keys - also gain unauthorized access. Such data shouldn't be publicly available.

Example e-mail

Such reports are sent by CERT PL to scanned entities
(but in Polish - Artemis supports translations).

Everything (besides finding a list of domains) is **fully automated!**

List of domains

- Customer database (if you're e.g. a hosting provider)
- Data portals: https://dane.gov.pl/en
- Tools such as crt.sh: https://crt.sh/?q=%25.gov.de,
- Custom databases (example: rspo.gov.pl for schools),
- Be creative (example: mamprawowiedziec.pl),
- (we use most of the above)

Who do we scan

Not only public entities!

- All gov.pl domains
- Local government
- Municipal corporations: water management, waste collection, …
- Cultural institutions
- Banks
- Universities, schools, preschools and other educational entities

Who do we scan

- Hospitals
- Local and country-level newspapers, TVs, information portals, etc.
- Websites of politicians, political parties, candidates, etc.
- Professional self-governments (e.g. medical chambers)
- Lists of domains provided e.g. by other CSIRTs or ministries
- **Everybody who wants it, for free**

Additional tool: Snitch

Idea: take a Shodan/FOFA dork and **send an e-mail to everybody in Poland that matches that dork.**

E.g.:

- exposed RDPs/VNCs
- exposed industrial control systems

Part 2: My CERT PL

One portal to rule them all

Why did we build the system?

Main motivation: incidents:

- caused by vulnerabilities,
- caused by leaked passwords.

Example: Polish Press Agency attack (fake news about military mobilization in Poland)

Additional motivation

- No legal basis to scan some sites.
- No information about some infrastructure (e.g. we know about the main university domain, but not about promotional domains).
- No contacts/bad ones for some website owners.
- Need to have multiple services in one place.
- We want to provide free scanning for everyone: small businesses, blog owners etc.

Services

- Scanning
- Network events
- Password leaks
- Security advisories
- Soon: attack surface intelligence

Used technology&data sources

- Scanning: **Artemis**
- Network events (e.g. hosts that host phishing or contact C&Cs): **n6, Shadowserver**
- Password leaks: **intelx.io, own threat hunting**
- The rest: **as boring as possible**
- *Choose boring technology*

Choose boring technology

- Django/PostgreSQL/k8s.
- No modern JS frameworks.
- Not a single-page app.

Demo

You are on moje.cert.pl

Log in to use CERT PL services that will increase the cybersecurity of your network and domains.

Log in

Create an account

Add domains

Domain names

Domain names

Each subsequent domain in a new line

Scan the security of systems in these domains

If you request a domain scan, its subdomains will also be scanned.
Security scanning will be performed using the Artemis system - see more .

Unblocking the firewall

If you are using a firewall or similar solution, we recommend whitelisting the following IP addresses to ensure complete scanning results (some devices may automatically block IP addresses that scan): 195.164.49.68 , 195.164.49.69 , 195.164.49.70 , 195.164.49.71 , and 195.164.49.72 .

Show advanced options

Add

Home page

example.com - password leaks

Show 10 position

Search:

Leak publication date	Description of the leak	Account	The first characters of the password	The page the person tried to log in to
2025-03-07	Credentials that were secured as a result of a law enforcement operation against Genesis Market (more information: https://policja.pl/pol/aktualnosci/230145,Policjanci-CBZC-w-miedzynarodowej-operacji-zamkniecia-przestepczego-serwisu-inte.html). The data was stolen using malware installed on users' computers - the presence of your data or your user's data in this leak means that it is highly likely that the user had malware installed on their equipment - please verify whether this problem still occurs.	example_username	Unknown	https://example.com

Scan results

example.com

Scanning from March 3, 2025 7:32 PM

The next scan will begin around **May 29, 2025** .

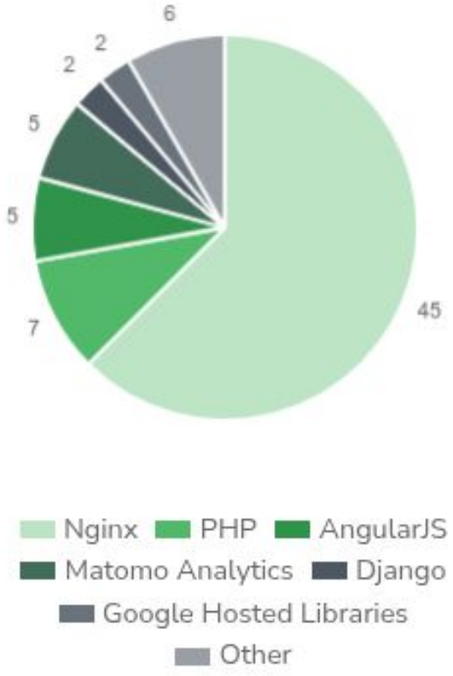
Low 2 Medium 1 High 0

Show 10 position

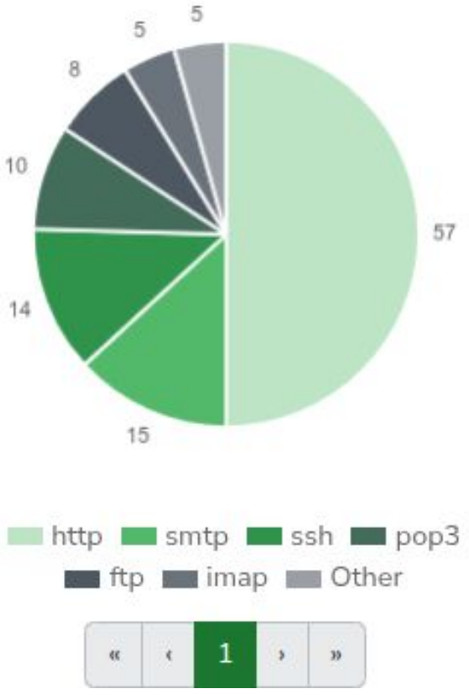
Search:

Severity	Resource	Vulnerability/Misconfiguration
Medium	example.com	The following domains do not have email sender verification mechanisms configured correctly: • example.com: No valid DMARC record found. We recommend using all three mechanisms: SPF, DKIM, and DMARC to reduce the chance that a spoofed message will be accepted by the recipient's server. Implementing these mechanisms will significantly increase the chance that the recipient's server will reject a forged email from the above domains. At https://bezpiecznapoczta.cert.pl you can verify the correct implementation of the sender verification mechanisms in your domain.

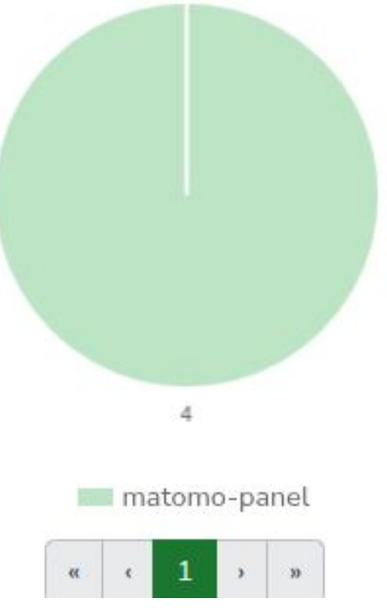
Identified technologies



Identified running services



Identified exposed administrative panels



Advisories

Receive by email | RSS

Read and unread | Any category | Filter

Notices for administrators

unread

November 22, 2025 7:18 PM

[58/2025] Vulnerability in Grafana Enterprise and Grafana Cloud

The CERT Polska team informs about a vulnerability in Grafana Enterprise and Grafana Cloud software: CVE-2025-41115.

Expand/Collapse | Mark as read

Notices for administrators

November 14, 2025 2:31 PM

[57/2025] Critical vulnerability actively exploited in Fortinet FortiWeb Manager appliances

The CERT Polska team informs about the CVE-2025-64446 vulnerability in FortiWeb software.

Expand/Collapse

Statistics

Statistics: scanning

- ~1.1M vulnerabilities and misconfigurations, including:
  - **~65k** high-severity,
  - **~687k** medium-severity,
  - **~409k** low-severity.
- For example we have more than **1700** confirmed SQL Injections (where we managed to **dump data from the database**).
- **>60% fixed vulnerabilities**

Statistics: My CERT.PL

- 14.5k users
- 17k verified domains
- 1.4k verified subnets

Aiming for more!

Example: SPF/DMARC

- **96%** having SPF, **79%** having DMARC

  Polish local government websites.

- **50%** having SPF, **15%** having DMARC

  Random sample of .com (having a website and existing at least 1 year).

What we learned from the users

- There was a huge need for such a project.
- What we consider a problem, they don't even notice. (And the other way around).

Part 3: Setting up a similar system

Why?

- There is a great need for security services for entities that don't have significant security budget.
- We can provide it for free because:
  - We have a dev team of **6 people** (and started with **2**)
  - We use an open source security scanner (**Artemis, using e.g. Nuclei and sqlmap**) and network feed data (**Shadowserver**).

Why?

- The permission to scan is given by the user (so no need to be government-backed).

  You can launch something similar as:

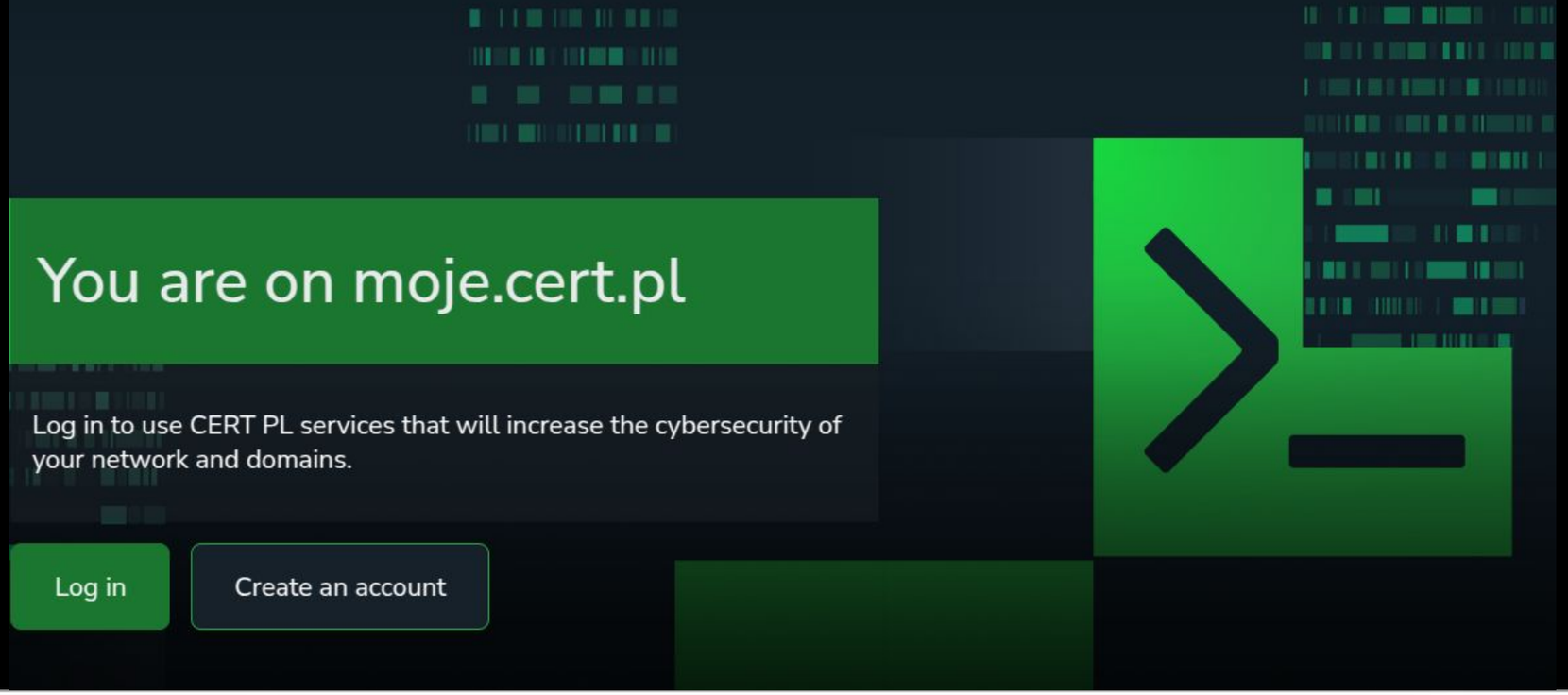
  - a hosting provider,
  - a NGO,
  - a group of enthusiasts.

How?

- Agile development
- Starting small
- Early launch
- **Bottom-up initiative**

  the bigger deal you make it, the more serious approvals you'll need.

Above worked for both Artemis and My CERT.PL.



Jesteś na moje.cert.pl

Zaloguj się, aby skorzystać z usług CERT Polska, które zwiększą cyberbezpieczeństwo Twojej sieci i domen.

Skanowanie

Możesz tu zamówić bezpłatne skanowanie bezpieczeństwa wszystkich Twoich domen.

Dotychczas CERT Polska przeskanował ok. 907 tys. domen i subdomen, na których znaleźliśmy ok. 475 tys. podatności i błędnych konfiguracji. Ok. 29 tys. z nich wiązało się w wysokim ryzykiem dla instytucji, której dotyczyły.

Wycieki haseł

CERT Polska będzie dla Ciebie wykrywać wycieki danych dotyczące użytkowników Twojej domeny. Jeśli wykryjemy że do niego doszło, zostaniesz o tym powiadomiony.

Zdarzenia w Twojej sieci

Infekcje złośliwym oprogramowaniem, a może inne zagrożenia dotyczące Twojej sieci? Jeśli jesteś administratorem sieci, to będziesz otrzymywać od CERT Polska informacje o takich zdarzeniach.

Zaloguj się

Utwórz konto

The funny parts

Scan reactions

A great initiative

Good morning,

First of all, thank you for launching this service, it's great.

Did I ask for such a scan? No.

So get the fuck out, you skunks. Mind your own business.

Bad bug fixing

- Hi, you have an SQL Injection. PoC: ?id=sleep(1)
- Thanks, we've fixed the bug
- Hello again, you still have an SQL Injection. PoC: ?id=sleeP(1)

Example: spoofed e-mails after multiple misconfigured SPF/DMARC warnings.

Takeaways

BlackHat Sound Bytes

Copy it

- Similar initiatives initiative can easily be set up in other countries.
- You don’t have to have access to significant resources.

Keep it simple

- The project isn’t sophisticated.
- Our approach combines multiple well-known open-source tools such as Nuclei and SQLmap.

It’s needed

- There is a huge need for such services, as demonstrated by the success of the presented initiative.
- Lots of low-hanging vulnerabilities.

Questions?