

CONFIDENTIAL · FREE ANALYSIS

FICTIONAL SAMPLE

CASE FILE · FREE-TARUMA-PAGOS-EXAMPLE

taruma-pagos.example.

Findings and fixes

METHOD	Passive reading of public data, no test on the systems
READ ON	2026-10-28 12:00 UTC
FINDINGS	2 high · 4 medium · 4 low · 4 informational
BASIS	Fictional company. Findings based on real analyses.

LOP.run



01 · WHAT WE FOUND

Findings in public data

14 confirmed findings: 2 high, 4 medium, 4 low, 4 informational.

RISK OVERVIEW

Findings by domain and severity

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Web	.	.	1	2	2	5
Server	.	.	1	.	.	1
Social	.	1	1	.	.	2
Email	.	.	1	1	1	3
Domain	.	1	.	1	1	3
TOTAL	0	2	4	4	4	14

ID	AREA	SEVERITY	SCORE
dns-dangling	subdomains	HIGH	8.2
leaks-staff	people	HIGH	8.1
email-dmarc	email	MEDIUM	6.1
web-js-cve	website	MEDIUM	6.1
brand-lookalikes	brand	MEDIUM	5.4
exposure-services	servers	MEDIUM	5.3
dns-dnssec	domain	LOW	3.7
email-mta-sts	email	LOW	3.7
web-cookies	website	LOW	3.1

ID	AREA	SEVERITY	SCORE
web-headers	website	LOW	3.1
dns-caa	domain	INFO	0.0
email-dmarc-rua	email	INFO	0.0
web-disclosure	website	INFO	0.0
web-security-txt	website	INFO	0.0

02 · THE FINDINGS

Each finding and its fix

Every finding carries the SHA-256 fingerprint of the public data we read on 2026-10-28. Ask us for those files and each one will match its fingerprint.

dns-dangling

There are subdomains pointing to services that no longer exist

CVSS 3.1

8.2

HIGH

DEPTH

INFO

LOW

MEDIUM

HIGH

CRITICAL

ID

dns-dangling

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/

UI:N/S:U/C:L/I:H/A:N

ASSET

subdomains

DOMAIN

Domain

STATUS

Confirmed

DESCRIPTION

1 subdomains point to an outside service that is no longer there: promo.taruma-pagos.example -> taruma-promo.herokuapp.com. On many of those services anyone can create an account with that name and take over the subdomain. It is a candidate: an authorized test confirms it.

BUSINESS IMPACT

Whoever takes over the subdomain can publish anything there in the company's name: a fake login page, malicious code or emails that pass the checks because they come from a real subdomain.

EVIDENCE FINGERPRINT

```
sha256:f5e42ebab00b8458e3b94bd7c0173f49eb808a52539ce2447a9f35b56a0d3d6e
```

HOW WE SAW IT

nslookup -type=CNAME <subdomain>

The target it returns does not exist (NXDOMAIN).

REMEDIATION

Delete from the DNS the records of subdomains no longer in use, or create the resource again on the outside service. Review the DNS every time a service is canceled.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

Leaks-staff

3 employee computers are infected with password-stealing programs

CVSS 3.1

8.1**HIGH**

DEPTH

INFO

LOW

MEDIUM

HIGH

CRITICAL

ID

Leaks-staff

VECTOR

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

ASSET

people

DOMAIN

Social

STATUS

Confirmed

DESCRIPTION

Hudson Rock's public database lists 3 computers of people with an @taruma-pagos.example email infected with password-stealing programs (infostealers); the latest one recorded is from 2026-08-14. We only took the count: we did not see or keep any password.

BUSINESS IMPACT

Those programs take every password saved in the browser, including the ones for the company's email, management system or bank. They are now one of the most common ways into a company without forcing anything.

EVIDENCE FINGERPRINT

```
sha256:c0152c404cae5c8c136d82439401f980e458617c1eb29af896d6bcacf80d29b39
```

HOW WE SAW IT

Look up the domain in Hudson Rock's free tool: <https://www.hudsonrock.com/free-tools>.

REMEDIATION

Change the passwords of every company account, starting with email, bank and admin; close open sessions; turn on two-step verification everywhere; and scan the computers with an antivirus, including the personal ones used for work.

WE CAN DO IT FOR YOU

Ears · US\$149 per month. We tell you about each new leak as soon as it shows up.

lop.run/en/services/ears

email-dmarc

Anyone can send email in the name of taruma-pagos.example

CVSS 3.1

6.1**MEDIUM**

DEPTH



ID

email-dmarc

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

ASSET

email

DOMAIN

Email

STATUS

Confirmed

DESCRIPTION

The domain has a DMARC policy in monitor-only mode (p=none). DMARC is the rule that tells mail servers around the world what to do with a message that claims to come from taruma-pagos.example but fails the checks. Without a policy that rejects or sets those messages aside, a third party can send email with a fake company sender and it will most likely land in the inbox.

BUSINESS IMPACT

An attacker can write to your customers, suppliers or employees as if they were someone at the company: invoices with changed bank details, urgent payment requests or links that steal passwords. The direct victims are the people who trust your emails, and the damage to the brand comes even though the company did nothing. It is closed with one DNS change, without touching the website or the mailbox.

EVIDENCE FINGERPRINT

```
sha256:d1cf02cef7f428f23754645f17a7337a8fc6bb3798a951807bab23d1c4c888f5
```

HOW WE SAW IT

Anyone can check it with a public DNS query, nslookup -type=TXT _dmarc.taruma-pagos.example. If there is no answer, or the answer says p=none, the domain does not ask other servers to reject fake email.

REMEDIATION

Move in three steps. (1) Publish DMARC with p=none and a reports mailbox (rua=mailto:...) to see who sends email on behalf of the domain. (2) Once every legitimate sender (company mail, billing system, newsletter tool) passes SPF or DKIM, raise it to p=quarantine. (3) After a few weeks without problems, move to p=reject.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

web-js-cve

The website loads libraries with known flaws

CVSS 3.1

6.1

MEDIUM

DEPTH

INFO

LOW

MEDIUM

HIGH

CRITICAL

ID

web-js-cve

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

ASSET

website

DOMAIN

Web

STATUS

Confirmed

DESCRIPTION

The home page loads these libraries in versions with published flaws: jQuery 3.4.1 (CVE-2020-11022). We see it from the file name and version; we did not test the flaw.

BUSINESS IMPACT

Several of these flaws let code run in the visitor's browser if the website uses the affected function: stealing sessions, changing what is shown or redirecting to a fake page.

EVIDENCE FINGERPRINT

```
sha256:7bc929995055e71404f556cde1e7baa7d415d096edc4781406252c023dcc0ba5
```

HOW WE SAW IT

View the home page source code and look for the script tags with those libraries.

REMEDIATION

Update each library to a fixed version (or remove it if it is no longer used) and test the website after the change.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

brand-lookalikes

There are domains almost identical to the company's, ready to send and receive email

CVSS 3.1

5.4**MEDIUM**

DEPTH

INFO	
LOW	
MEDIUM	
HIGH	
CRITICAL	

ID

brand-lookalikes

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

ASSET

brand

DOMAIN

Social

STATUS

Confirmed

DESCRIPTION

We found 1 registered domains that look like taruma-pagos.example and have email set up: tarumapagos.example. They may be legitimate (from the same company or another one with a similar name); from the outside you cannot tell who owns them.

BUSINESS IMPACT

A domain with one letter changed and working email is the classic tool of invoice fraud: the customer gets an email that seems to come from the company, from an almost identical address, with new bank details.

EVIDENCE FINGERPRINT

```
sha256:ef98345799def75fe08b7e16381f9d37d4c3d1957cb68dad  
e3b470c547212624
```

HOW WE SAW IT

Look up each domain at <https://lookup.icann.org> and its email with `nslookup -type=MX <domain>`.

REMEDIATION

Check who owns each domain. Keep your own ones without email or redirect them. For the others, tell customers and suppliers that the company never changes bank details by email and, if there is malicious use, ask the registrar to take it down.

WE CAN DO IT FOR YOU

Whisker · US\$1,900. We train your team for this impersonation.

lop.run/en/services/whisker

exposure-services

There are services open to the internet besides the website

CVSS 3.1

5.3**MEDIUM**

DEPTH

INFO	
LOW	
MEDIUM	
HIGH	
CRITICAL	

ID

exposure-services

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

ASSET

servers

DOMAIN

Server

STATUS

Confirmed

DESCRIPTION

Shodan's public index lists these services on the domain's servers besides the web: 203.0.113.24 (22). We did not scan anything: this is what Shodan already published.

BUSINESS IMPACT

Each open service (remote access, databases, admin panels) is one more door that can be attacked by password or through a software flaw. Many automated attacks sweep the internet looking for exactly these ports.

EVIDENCE FINGERPRINT

```
sha256:ef2a4a0818149e830fd69e8cb6ee7f2b04bc52576fb2b5665  
fec6e1495bdcea5
```

HOW WE SAW IT

Check each address at <https://internetdb.shodan.io/<IP>> or on shodan.io.

REMEDIATION

Close at the firewall every port that does not need to be public; keep remote access and databases only behind a VPN or a list of allowed addresses.

WE CAN DO IT FOR YOU

Dig · US\$4,500. We check it from the inside, with your signed authorization.

lop.run/en/services/dig

03 · LOWER SEVERITY

Low and informational

LOW

CVSS 3.7 dns-dnssec domain · Domain

The domain's DNS answers are not signed (DNSSEC)

DESCRIPTION

taruma-pagos.example does not have DNSSEC turned on. DNSSEC signs DNS answers so whoever asks can check that the address of the website or the mail server is the one the company published, not one forged along the way.

BUSINESS IMPACT

Without a signature, an attacker who manages to poison an intermediate DNS server can send visitors or email to a server of their own. It is an uncommon attack, and turning DNSSEC on is usually an option at the domain provider.

EVIDENCE FINGERPRINT

```
sha256:ffa6e41201b4fb6d13478acb9a85d395e9968dbfcb3a63cce70703d18be0f476
```

HOW WE SAW IT

Check the domain in a public DNSSEC validator (for example dnsviz.net) or ask the DNS for the DS record:

```
nslookup -type=DS taruma-pagos.example
```

REMEDIATION

Turn on DNSSEC at the DNS provider and, if the DNS and the domain registration are with different companies, add the DS record at the registrar. Check it afterwards with a public validator.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

LOW

CVSS 3.7 email-mta-sts email · Email

Email the company receives can travel without encryption

DESCRIPTION

The domain has no MTA-STS policy in enforce mode, or has no TLS-RPT. MTA-STS requires other servers to deliver email for taruma-pagos.example only over an encrypted, verified connection; TLS-RPT reports when that delivery fails.

BUSINESS IMPACT

Someone with access to the network the email crosses can force messages to travel without encryption and read them. It is a hard attack, but company email carries invoices, contracts and passwords.

EVIDENCE FINGERPRINT

```
sha256:15a55832a5c2519ab65d0f7222b4586defb25bf76aec3163b68831a1f785b95a
```

HOW WE SAW IT

```
nslookup -type=TXT _mta-sts.taruma-pagos.example nslookup -type=TXT _smtp._tls.taruma-pagos.example
```

If there is no answer, the policy or the report is missing.

REMEDIATION

Publish the policy file at <https://mta-sts.taruma-pagos.example/.well-known/mta-sts.txt>, first in testing mode, together with the _mta-sts record and the TLS-RPT record with a reports mailbox. Move to enforce mode when the reports show no failures.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

LOW

CVSS 3.1 web-cookies website · Web

The website hands out cookies without the basic protections

DESCRIPTION

The home page hands out 1 cookies without the Secure flag or without the HttpOnly flag. The Secure flag stops them from traveling without encryption; the HttpOnly flag stops malicious code on the page from reading them.

BUSINESS IMPACT

If one of those cookies identifies a user's session, a minor bug in the website is enough to steal it and get into their account.

EVIDENCE FINGERPRINT

```
sha256:81dbaf68e0168a38704c43da233efb9e9347d20afd9667fc1071c570b2367d16
```

HOW WE SAW IT

In the browser developer tools, Application (or Storage) tab, check the Secure and HttpOnly columns of each cookie.

REMEDIATION

Mark every cookie with Secure and SameSite=Lax, and session cookies also with HttpOnly. In most systems it is a configuration option.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

LOW

CVSS 3.1 web-headers website · Web

The website is missing its basic security headers

DESCRIPTION

The home page does not send these headers: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options. They are instructions the website gives the browser to limit what code can run, whether the page can be placed inside another one and how to read the files.

BUSINESS IMPACT

They are not a flaw on their own, but without them a bug in the website (a badly validated form, a vulnerable plugin) becomes much easier to use against visitors.

EVIDENCE FINGERPRINT

```
sha256:1501c3f97d6b5371caad8a1deb696247ef0fb517db615d7ac717fdfa083be4c3
```

HOW WE SAW IT

Look at the headers of the response from <https://taruma-pagos.example> in the browser developer tools (Network tab).

REMEDIATION

Add X-Content-Type-Options: nosniff and X-Frame-Options: SAMEORIGIN (so the page only shows inside the same website), and build a Content-Security-Policy starting in report-only mode so the website does not break.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

INFO

CVSS 0.0 dns-caa domain · Domain

Nothing restricts who can issue certificates for the domain

DESCRIPTION

taruma-pagos.example has no CAA records. A CAA record says which certificate authorities may issue certificates for the domain; without it, any of them can.

BUSINESS IMPACT

It is an extra layer: it lowers the chance that someone gets a valid certificate for the domain by fooling a careless authority.

EVIDENCE FINGERPRINT

```
sha256:cdd9c82c1f0ab4746ff0f570ddcb68cfbeb3152453ea7e7a2301a4abcad25639
```

HOW WE SAW IT

```
nslookup -type=CAA taruma-pagos.example
```

REMEDIATION

Publish a CAA record that allows only the authority that already issues the website's certificates (for example Let's Encrypt) and names a mailbox for notices.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

INFO

CVSS 0.0 email-dmarc-rua email · Email

Nobody receives the reports on who uses the domain's name

DESCRIPTION

The DMARC policy of taruma-pagos.example does not name a reports mailbox (the RUA tag). The large email providers send that mailbox a daily summary of the messages that claim to come from the domain, legitimate and fake.

BUSINESS IMPACT

Without those reports the company does not find out if someone is sending email in its name, and has no data to tighten the policy without cutting off its own sending.

EVIDENCE FINGERPRINT

```
sha256:d4cfc079679fecc5e896869085b8a35666797cb29409918c2cc5819a532e0880
```

HOW WE SAW IT

The answer to `nslookup -type=TXT _dmarc.taruma-pagos.example` has no `rua=` tag, the one that says where to send the reports.

REMEDIATION

Add `rua=mailto:dmarc@taruma-pagos.example` (or the mailbox of a DMARC report analysis service) to the DMARC record and review the reports once a week.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

INFO

CVSS 0.0 web-disclosure website · Web

The website announces which software and version it runs

DESCRIPTION

The website's response announces the software and its version (Server: nginx/1.18.0). With the exact version, anyone can look up the known flaws of that software without testing anything.

BUSINESS IMPACT

It is not a flaw, but it saves work for whoever hunts for websites running a vulnerable version to attack them in bulk.

EVIDENCE FINGERPRINT

```
sha256:eaea0ab950a5eb7d0a2285c19738060c24714ee8abfd6c244035a35359aeda86
```

HOW WE SAW IT

Look at the response headers and, in the home page source code, the tag that announces what the website was built with.

REMEDIATION

Remove the version from the server headers and from that tag, and keep the software updated, which is what actually protects you.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

INFO

CVSS 0.0 web-security-txt website · Web

There is no published contact for reporting security flaws

DESCRIPTION

The website has no /.well-known/security.txt file. It is the standard place (RFC 9116) where a researcher looks for whom to tell after finding a flaw.

BUSINESS IMPACT

Whoever finds a problem and does not know whom to write to usually publishes it or drops it. With a clear contact, the company hears first.

EVIDENCE FINGERPRINT

```
sha256:263dbad276b48f0dfa763b12ea111a043ebdf5ab3fc8824eca09c2a96cf88d31
```

HOW WE SAW IT

Open <https://taruma-pagos.example/.well-known/security.txt>: it does not exist.

REMEDIATION

Publish /.well-known/security.txt with at least Contact: <mailto:security@taruma-pagos.example> and Expires: with a date within the next year.

WE CAN DO IT FOR YOU

Lop Fix · US\$95 per hour (minimum US\$150). We fix it by the hour or at a fixed price.

lop.run/en/services/lop-fix

04 · NEXT STEPS

What this analysis does not look at

This analysis reads only public data from taruma-pagos.example: it does not get into your website or your systems. What is inside is what an audit looks at, with your signed authorization:

US\$4,500

Dig

Your website and your servers tested from the inside: the login, the forms, the payments and what runs behind them.

lop.run/en/services/dig

US\$9,500

Rabbit Hole

Your whole platform: each customer's accounts and permissions, the APIs, the business logic and the cloud.

lop.run/en/services/rabbit-hole

from US\$15,000

Warren

Your whole company: besides the platform, the office network, the Wi-Fi, the email and whether your team falls for a scam.

lop.run/en/services/warren

US\$490

Sniff

Not sure which one you need? A specialist goes over this analysis with you for 30 minutes and tells you, at a fixed price. If you then hire an audit, it is credited.

lop.run/en/services/sniff

What you can do now

Free

Monitoring badge

We check your domain once a month, at no cost, and write to you only if something changed.

lop.run/en/services/#free

US\$449 per month

Ears + Lop

We watch your domain around the clock and a specialist confirms every alert before it reaches you and tells you what to do. This analysis found serious findings: with a person beside you, you do not depend on reading each alert yourself.

lop.run/en/services/ears-lop

US\$95 per hour (minimum US\$150)

Lop Fix

This report has 11 configuration fixes. If you would rather not do them yourself, we do them for you.

lop.run/en/services/lop-fix

FINDINGS AND FIXES

Prepared for taruma- pagos.example.

This analysis read only public data from taruma-pagos.example on 2026-10-28. Nobody tested or touched your systems. If you want legal advice on these obligations, we can put you in touch with specialized lawyers.