

CONFIDENCIAL · ANÁLISE GRÁTIS

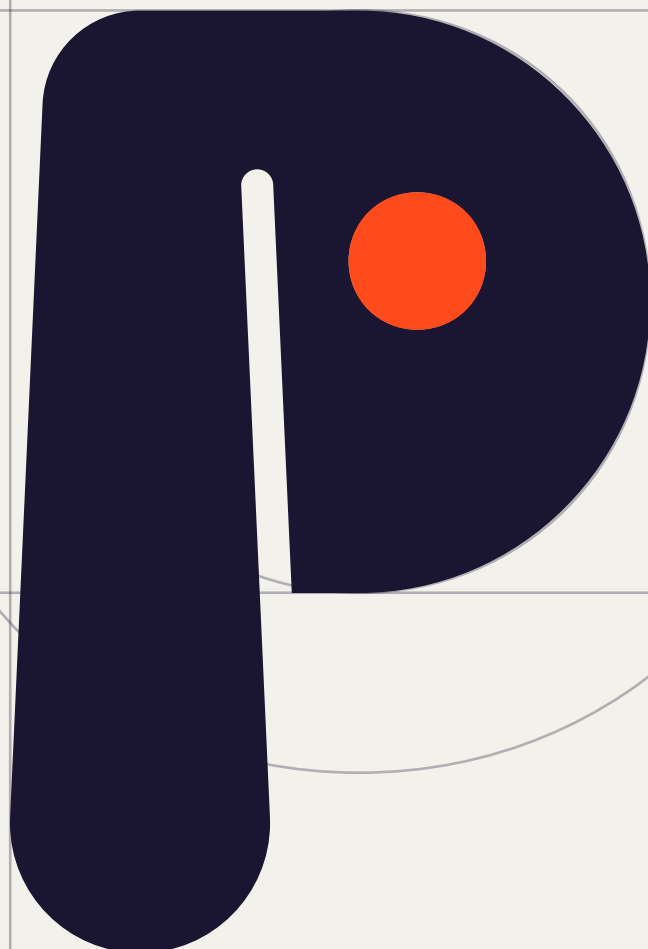
EXEMPLO FICTÍCIO

DOSSIÊ · FREE-TARUMA-PAGOS-EXAMPLE

taruma-pagos.example.

Resumo para a diretoria

MÉTODO	Leitura passiva de dados públicos, sem testes nos sistemas
LIDO EM	2026-10-28 12:00 UTC
ACHADOS	2 altas · 4 médias · 4 baixas · 4 informativas
ORIGEM	Empresa fictícia. Achados baseados em análises reais.



01 · O RISCO NUM RELANCE

O que está em jogo

14 achados confirmados: 2 altas, 4 médias, 4 baixas, 4 informativas.

PANORAMA DE RISCO

Achados por domínio e severidade

	CRÍTICA	ALTA	MÉDIA	BAIXA	INFO	TOTAL
Web	.	.	1	2	2	5
Servidor	.	.	1	.	.	1
Social	.	1	1	.	.	2
E-mail	.	.	1	1	1	3
Domínio	.	1	.	1	1	3
TOTAL	0	2	4	4	4	14

ACHADO	ÁREA	SEVERIDADE	NOTA
Há subdomínios que apontam para serviços que não existem mais	subdomínios	ALTA	8.2
Há 3 computadores de funcionários infectados com programas que roubam senhas	peessoas	ALTA	8.1
Qualquer pessoa pode enviar e-mails se passando por taruma-pagos.example	e-mail	MÉDIA	6.1
O site carrega bibliotecas com falhas conhecidas	site	MÉDIA	6.1
Há domínios quase iguais ao da empresa prontos para receber e enviar e-mail	marca	MÉDIA	5.4
Há serviços abertos à internet além do site	servidores	MÉDIA	5.3
As respostas do DNS do domínio não são assinadas (DNSSEC)	domínio	BAIXA	3.7
O e-mail que a empresa recebe pode trafegar sem criptografia	e-mail	BAIXA	3.7

ACHADO	ÁREA	SEVERIDADE	NOTA
O site entrega cookies sem as proteções básicas	site	BAIXA	3.1
Faltam os cabeçalhos de segurança básicos do site	site	BAIXA	3.1
Não há restrição de quem pode emitir certificados para o domínio	domínio	INFO	0.0
Ninguém recebe os relatórios de quem usa o nome do domínio	e-mail	INFO	0.0
O site anuncia qual software e versão usa	site	INFO	0.0
Não há um contato publicado para avisar sobre falhas de segurança	site	INFO	0.0

02 · EM TERMOS DE NEGÓCIO

Os achados para a diretoria

Achado 1 de 14

Há subdomínios que apontam para serviços que não existem mais

CVSS 3.1

8.2**ALTA**

PROFUNDIDADE

INFO	
BAIXA	
MÉDIA	
ALTA	
CRÍTICA	

ÁREA

subdomínios

DOMÍNIO

Domínio

O QUE ESTÁ EM JOGO

Quem ficar com o subdomínio pode publicar ali o que quiser com o nome da empresa: uma página falsa de acesso, código malicioso ou e-mails que passam nas verificações por virem de um subdomínio real.

Achado 2 de 14

Há 3 computadores de funcionários infectados com programas que roubam senhas

CVSS 3.1

8.1

ALTA

PROFUNDIDADE

INFO

BAIXA

MÉDIA

ALTA

CRÍTICA

ÁREA

pessoas

DOMÍNIO

Social

O QUE ESTÁ EM JOGO

Esses programas levam todas as senhas salvas no navegador, incluindo as do e-mail, do sistema de gestão ou do banco da empresa. Hoje são uma das formas mais comuns de entrar em uma empresa sem forçar nada.

EXPOSIÇÃO FINANCEIRA

Acesso com senhas roubadas

O custo depende de quais contas eram usadas nesses computadores: e-mail, banco, sistemas internos.

EXPOSIÇÃO LEGAL E REGULATÓRIA

Se essas contas forem usadas para acessar dados pessoais de clientes ou funcionários, pode surgir a obrigação de comunicar a autoridade de proteção de dados de cada país.

Orientativo: não constitui assessoria jurídica.

Achado 3 de 14

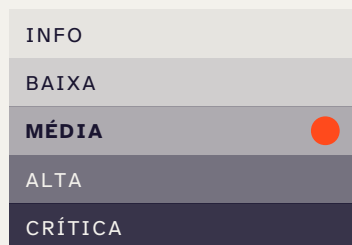
Qualquer pessoa pode enviar e-mails se passando por taruma-pagos.example

CVSS 3.1

6.1

MÉDIA

PROFUNDIDADE



ÁREA

e-mail

DOMÍNIO

E-mail

O QUE ESTÁ EM JOGO

Um atacante pode escrever para seus clientes, fornecedores ou funcionários como se fosse alguém da empresa: boletos e faturas com dados bancários trocados, pedidos de pagamento urgentes ou links para roubar senhas. As vítimas diretas são as pessoas que confiam nos seus e-mails, e o dano à marca chega mesmo que a empresa não tenha feito nada. Resolve-se com uma mudança no DNS, sem mexer no site nem no e-mail.

EXPOSIÇÃO FINANCEIRA

Fraude por e-mail falso

A perda típica é o valor do boleto, da fatura ou do pagamento desviado, mais o custo de recuperar a confiança de quem recebeu o e-mail.

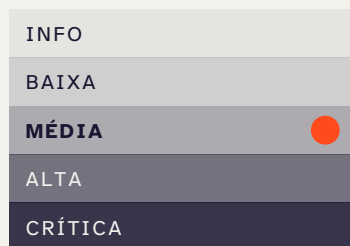
Achado 4 de 14

0 site carrega bibliotecas com falhas conhecidas

CVSS 3.1

6.1**MÉDIA**

PROFUNDIDADE



ÁREA

site

DOMÍNIO

Web

O QUE ESTÁ EM JOGO

Várias dessas falhas permitem rodar código no navegador do visitante se o site usar a função afetada: roubar sessões, alterar o que é mostrado ou redirecionar para uma página falsa.

Achado 5 de 14

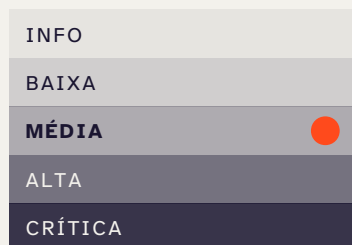
Há domínios quase iguais ao da empresa prontos para receber e enviar e-mail

CVSS 3.1

5.4

MÉDIA

PROFUNDIDADE



ÁREA

marca

DOMÍNIO

Social

O QUE ESTÁ EM JOGO

Um domínio com uma letra trocada e e-mail ativo é a ferramenta clássica do golpe do boleto e da fatura: o cliente recebe um e-mail que parece da empresa, de um endereço quase idêntico, com dados bancários novos.

EXPOSIÇÃO FINANCEIRA

Fraude por e-mail falso

A perda típica é o valor do boleto, da fatura ou do pagamento desviado.

Achado 6 de 14

Há serviços abertos à internet além do site

CVSS 3.1

5.3**MÉDIA**

PROFUNDIDADE

INFO	
BAIXA	
MÉDIA	●
ALTA	
CRÍTICA	

ÁREA

servidores

DOMÍNIO

Servidor

O QUE ESTÁ EM JOGO

Cada serviço aberto (acesso remoto, bancos de dados, painéis) é mais uma porta que pode ser atacada por senha ou por uma falha do software. Muitos ataques automáticos percorrem a internet procurando justamente essas portas.

03 · SEVERIDADE MENOR

Baixas e informativas

BAIXA CVSS 3.7 Achado 7 de 14 domínio · Domínio

As respostas do DNS do domínio não são assinadas (DNSSEC)

O QUE ESTÁ EM JOGO

Sem assinatura, um atacante que consiga envenenar um servidor DNS intermediário pode mandar os visitantes ou o e-mail para um servidor dele. É um ataque pouco comum, e ativar o DNSSEC costuma ser uma opção do provedor do domínio.

BAIXA CVSS 3.7 Achado 8 de 14 e-mail · E-mail

O e-mail que a empresa recebe pode trafegar sem criptografia

O QUE ESTÁ EM JOGO

Alguém com acesso à rede por onde passa o e-mail pode forçar que as mensagens trafeguem sem criptografia e lê-las. É um ataque difícil, mas o e-mail de uma empresa leva faturas, contratos e senhas.

BAIXA CVSS 3.1 Achado 9 de 14 site · Web

O site entrega cookies sem as proteções básicas

O QUE ESTÁ EM JOGO

Se um desses cookies identifica a sessão de um usuário, uma falha menor no site basta para roubá-lo e entrar na conta dele.

BAIXA CVSS 3.1 Achado 10 de 14 site · Web

Faltam os cabeçalhos de segurança básicos do site

O QUE ESTÁ EM JOGO

Não são uma falha por si só, mas sem eles um erro no site (um formulário mal validado, uma extensão vulnerável) fica muito mais fácil de explorar contra os visitantes.

INFO

CVSS 0.0 Achado 11 de 14 domínio · Domínio

Não há restrição de quem pode emitir certificados para o domínio

O QUE ESTÁ EM JOGO

É uma camada extra: reduz a chance de alguém conseguir um certificado válido para o domínio enganando uma autoridade descuidada.

INFO

CVSS 0.0 Achado 12 de 14 e-mail · E-mail

Ninguém recebe os relatórios de quem usa o nome do domínio

O QUE ESTÁ EM JOGO

Sem esses relatórios a empresa não fica sabendo se alguém está enviando e-mails em seu nome, e não tem dados para endurecer a política sem cortar envios próprios.

INFO

CVSS 0.0 Achado 13 de 14 site · Web

O site anuncia qual software e versão usa

O QUE ESTÁ EM JOGO

Não é uma falha, mas poupa trabalho para quem procura sites com uma versão vulnerável para atacá-los em massa.

INFO

CVSS 0.0 Achado 14 de 14 site · Web

Não há um contato publicado para avisar sobre falhas de segurança

O QUE ESTÁ EM JOGO

Quem encontra um problema e não sabe a quem escrever costuma publicá-lo ou deixá-lo de lado. Com um contato claro, a empresa fica sabendo primeiro.

04 · PRÓXIMOS PASSOS

0 que esta análise não olha

Esta análise lê só dados públicos de taruma-pagos.example: não entra no seu site nem nos seus sistemas. O que há por dentro é o que uma auditoria olha, com a sua autorização assinada:

US\$4.500

Dig

O seu site e os seus servidores testados por dentro: o login, os formulários, os pagamentos e o que roda por trás.

lop.run/pt-br/servicos/dig

US\$9.500

Rabbit Hole

A sua plataforma inteira: as contas e as permissões de cada cliente, as APIs, a lógica do negócio e a nuvem.

lop.run/pt-br/servicos/rabbit-hole

a partir de US\$15.000

Warren

A sua empresa inteira: além da plataforma, a rede do escritório, o wi-fi, o e-mail e se a sua equipe cai em um golpe.

lop.run/pt-br/servicos/warren

US\$490

Sniff

Não sabe qual precisa? Um especialista olha esta análise com você por 30 minutos e diz, com preço fechado. Se depois você contratar uma auditoria, o valor é descontado.

lop.run/pt-br/servicos/sniff

O que você pode fazer agora

Grátis

Selo de monitoramento

Revisamos o seu domínio uma vez por mês, sem custo, e escrevemos só se algo mudou.

lop.run/pt-br/servicos/#gratis

US\$449 por mês

Ears + Lop

Vigiamos o seu domínio 24 horas por dia e um especialista confirma cada alerta antes que ele chegue a você e diz o que fazer. Esta análise encontrou achados graves: com uma pessoa ao lado você não depende de interpretar cada alerta.

lop.run/pt-br/servicos/ears-lop

US\$95 por hora (mínimo US\$150)

Lop Fix

Este relatório traz 11 correções de configuração. Se preferir não fazê-las você mesmo, fazemos por você.

lop.run/pt-br/servicos/lop-fix

RESUMO PARA A DIRETORIA

Preparado para taruma- pagos.example.

Esta análise leu só dados públicos de taruma-pagos.example em 2026-10-28. Ninguém testou nem tocou nos seus sistemas. Se quiser assessoria jurídica sobre essas obrigações, podemos colocar você em contato com advogados especializados.