

Threat Model for a Precision Agriculture System

Henrique Faria A82200 and Paulo Rosa A81139

Departamento de Informática, Universidade do Minho

Resumo Este trabalho tem como objetivo reportar as informações recolhidas no âmbito do estudo de duas empresas, uma de grandes dimensões e uma de pequenas dimensões.

Para a realização da recolha de informações foram feitas pesquisas no google sobre a empresa visada, consultaram-se os respetivos portais na internet e descarregu-se com recurso ao comando *wget* as respetivas páginas sendo estas analisadas visando revelar informações guardadas como anotações, e fizeram-se queries com os comandos *dig* e *whois* acerca dos servidores responsáveis pela footprint da empresa na internet. Para além disso pode também ser consultado o site para obter informações que digam respeito às tecnologias usadas em páginas antigas ou ao próprio código modificado.

Também se recorreu ao uso de ferramentas como o *open port finder* online, o comando *host* e o *zenMap* para auxiliar o footprinting das empresas. Neste são especificados os tipos de dados que se podem pretender obter com um ataque à empresa e como estes são tratados. Também são referidos contactos de telemóvel, telefone, emails e localizações consideradas pertinentes. No fim exibem-se queries feitas aos servidores e as respostas obtidas sendo prossecutidas por uma breve explicação.

Palavras-chave: Wget · Whois · Dig · Open Port Finder · Host · ZenMap · Pingo Doce · Gamingreplay

1 Dados Sensíveis

"Dados como nome, morada e número de contribuinte são mantidos pelo período definido por lei após a faturação."

"Dados pessoais necessários para realizar candidaturas ou donativos são também guardados até ao final do processo para os quais foram dados. Após isso são eliminados."

Por estas citações podemos concluir que caso ganhemos acesso ao sistema, conseguiremos obter nomes, moradas, números de contribuintes e outros dados sensíveis.

1.1 Fragilidades na Comunicação de Dados Pessoais e Segurança

"A Companhia recorre a parceiros externos nomeadamente para desenvolvimento, manutenção e alojamento de sistemas informáticos, agências de marketing e comunicação, estudos de mercado, apoio ao cliente, a triagem, avaliação e selecção de candidatos. Nestes casos, a Companhia assegura que os seus parceiros cumprem com as medidas técnicas e organizacionais adequadas à actividade de processamento. Neste âmbito, os dados recolhidos poderão ser transferidos para entidades que se localizam em países terceiros (fora da União Europeia), sendo assegurado que são tomadas as medidas de segurança apropriadas de acordo com a legislação em vigor."

Segundo esta citação os dados pessoais dos utilizadores podem ser enviados a terceiros aumentando as chances de um atacante poder obter esses dados durante a transferência dos mesmos. Para além disso as políticas de segurança de uma empresa "parceira" do pinga doce ainda que submetida à legislação em vigor, pode ter critérios de segurança pouco firmes por exemplo no requisito de impedir ataques por engenharia social.

Note-se que uma das melhores formas de obter dados sensíveis de uma empresa de grande dimensão é muitas vezes fazendo uso de parceiros de menor dimensão com critérios de segurança mais lassos.

2 Autenticação - Facebook ou Google

O utilizador da plataforma pode usar uma conta Google ou de Facebook para se autenticar na plataforma, isto acrescenta vulnerabilidades no acesso aos dados do utilizador visto que podemos atacar outros sistemas para além deste, que podem ter outras vulnerabilidades.

Por exemplo, o facebook, caso um utilizador se engane a escrever a password e apenas altere uma letra muitas vezes assume que se trata da pessoa certa e permite o acesso à conta.

3 Contactos Importantes

- Correio electrónico para clientes: cliente@pingodoce.pt
- Telemóvel: 808 204 545
- Telefone: 210 114 411
- Linha de registo cartão poupa mais: 707 50 20 69
- Localização sede:

Av. Santo Condestável – Via Central Chelas 1900-806 Lisboa

- Localização do departamento de recursos humanos:

Pingo Doce Distribuição Alimentar SA., Rua Actor António Silva, 7 – 6º
1649-033 Lisboa

- CEO pingo doce: Isabel Ferreira Pinto

Perfil Linkdin: <https://www.linkedin.com/in/isabel-ferreira-pinto-73b88046/>

- Perfis de funcionários úteis para "social engieniering":

<https://www.linkedin.com/company/pingo-doce/people/>

- Email do encarregado de Protecção de Dados: dpo.portugal@jeronimo-martins.com

4 Querys para obter informações sobre servidores e serviços

4.1 dig -4 www.pingodoce.pt

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
;; QUESTION SECTION:
;www.pingodoce.pt. IN A

;; ANSWER SECTION:
www.pingodoce.pt. 44 IN A 194.65.31.215

;; AUTHORITY SECTION:
pingodoce.pt. 44 IN NS dns3.pingodoce.pt.
```

```
pingodoce.pt. 44 IN NS dns2.pingodoce.pt.
pingodoce.pt. 44 IN NS dns.pingodoce.pt.
```

```
:: ADDITIONAL SECTION:
dns3.pingodoce.pt. 44 IN A 213.13.169.10
dns.pingodoce.pt. 44 IN A 194.65.31.202
dns2.pingodoce.pt. 44 IN A 194.65.31.203

;; Query time: 52 msec
;; SERVER: 193.137.16.65#53(193.137.16.65)
;; WHEN: Mon Oct 28 10:05:15 WET 2019
;; MSG SIZE rcvd: 165
```

Note-se que só é apresentado o dig -4 e não o dig -6 pois não há resposta de nenhum servidor quando inquirimos *www.pingodoce.pt* com IPv6.

Como podemos ver pela resposta obtida pelo dig temos 3 NameServers autoritários para *www.pingodoce.pt*:

- dns3.pingodoce.pt
- dns2.pingodoce.pt
- dns.pingodoce.pt

Estes têm respetivamente os seguintes endereços IPv4:

- 213.13.169.10
- 194.65.31.203
- 194.65.31.202

O endereço destino *www.pingodoce.pt* tem IPv4 194.65.31.215.

Podemos concluir sobre os IPs que dois dos nomes autoritários partilham a mesma rede do endereço alvo (194.65.31.X/24) e um terceiro servidor, dns3.pingodoce.pt, encontra-se numa rede separada (213.13.169.X/24).

4.2 Whois pingodoce.pt

Domain: pingodoce.pt
Domain Status: Registered

Creation Date: 04/06/1998 00:00:00
Expiration Date: 04/07/2022 23:59:40

Owner Name: Pingo Doce - Distribuicao Alimentar S.A.
Owner Address: Rua Actor Antonio Silva, 7
Owner Locality: LISBOA
Owner ZipCode: 1649-033

Owner Locality ZipCode: LISBOA
Owner Country Code: PT
Owner Email:
dsiacounts@jeronimo-martins.pt,dsiacounts@jeronimo-martins.com

Admin Name: Pingo Doce - Distribuicao Alimentar S.A.
Admin Address: Rua Actor Antonio Silva, 7
Admin Locality: LISBOA
Admin ZipCode: 1649-033
Admin Locality ZipCode: LISBOA
Admin Country Code: PT
Admin Email:
dsiacounts@jeronimo-martins.pt,dsiacounts@jeronimo-martins.com

Name Server: dns2.pingodoce.pt | IPv4: 194.65.31.203 and IPv6:
Name Server: dns3.pingodoce.pt | IPv4: 213.13.169.10 and IPv6:
Name Server: dns.pingodoce.pt | IPv4: 194.65.31.202 and IPv6:

Com o comando *whois pingodoce.pt* obtemos mais algumas informações sobre quem estamos a investigar.
Estas informações são sobre as datas de criação e em que expira o dominio, sobre o dono sabemos o nome, a localização da sua sede, o código postal, o país e o email do mesmo. Para além disso temos análogas sobre o administrador do sistema.
Apesar de usar o *whois* nos fornecer estes dados extra de formos a <https://www.iana.org/whois> e pesquisarmos por *www.pingodoce.pt* podemos obter informação sobre quem registou este site, neste caso os responsáveis pelo dominio *.pt*. O resultado segue em baixo.

```

% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.dns.pt

domain:     PT

organisation: Associação DNS.PT
address:    Rua Latino Coelho, nº13, 5º piso
address:    1050-132 Lisboa
address:    Portugal

contact:    administrative
name:       Luisa Lopes Gueifão
organisation: Associação DNS.PT
address:    Rua Latino Coelho, nº13, 5º piso
address:    1050-132 Lisboa
address:    Portugal
phone:      (+351) 211308200
fax-no:     (+351) 211312720
e-mail:     lgueifao@dns.pt

contact:    technical
name:       Eduardo Manuel Laureano Duarte
organisation: Associação DNS.PT
address:    Rua Latino Coelho, nº13, 5º piso
address:    1050-132 Lisboa
address:    Portugal
phone:      (+351) 211308200
fax-no:     (+351) 211312720
e-mail:     eduardo.duarte@dns.pt

nserver:    A.DNS.PT 185.39.208.1 2a04:6d80:0:0:0:0:1
nserver:    B.DNS.PT 194.0.25.23 2001:678:20:0:0:0:0:23
nserver:    C.DNS.PT 2001:500:14:6105:ad:0:0:1 204.61.216.105
nserver:    D.DNS.PT 185.39.210.1 2a04:6d82:0:0:0:0:0:1
nserver:    E.DNS.PT 193.136.192.64 2001:690:a00:4001:0:0:0:64
nserver:    F.DNS.PT 162.88.45.1 2600:2000:3009:0:0:0:0:1
nserver:    G.DNS.PT 193.136.2.226 2001:690:a80:4001:0:0:0:100
nserver:    NS.DNS.BR 200.160.0.5 2001:12ff:0:a20:0:0:0:5
nserver:    NS2.NIC.FR 192.93.0.4 2001:660:3005:1:0:0:1:2
nserver:    SNS-PB.ISC.ORG 192.5.4.1 2001:500:2e:0:0:0:0:1
ds-rdata:   40995 7 2 ABF415ED56E88C5F05434BBF62CDD90B574D6445A37AE5CC9B84638AB5B9E656
ds-rdata:   40995 7 1 43DEDCEEBA41380680784AA531819A6ED8172B6D

whois:      whois.dns.pt

status:     ACTIVE
remarks:    Registration information: http://www.dns.pt/

created:    1988-06-30
changed:    2018-08-10
source:     IANA

```

Figura 1. Dados do registador do site www.pingodoce.pt

Este resultado é útil na medida em que revela nomes, emails, números de telefone etc.

Posteriormente foram testadas algumas portas para o IP 194.65.31.215 referente a www.pingodoce.pt. A seguinte imagem representa a busca feita a várias portas conhecidas que se enumeram de seguida bem como os respetivos resultados.

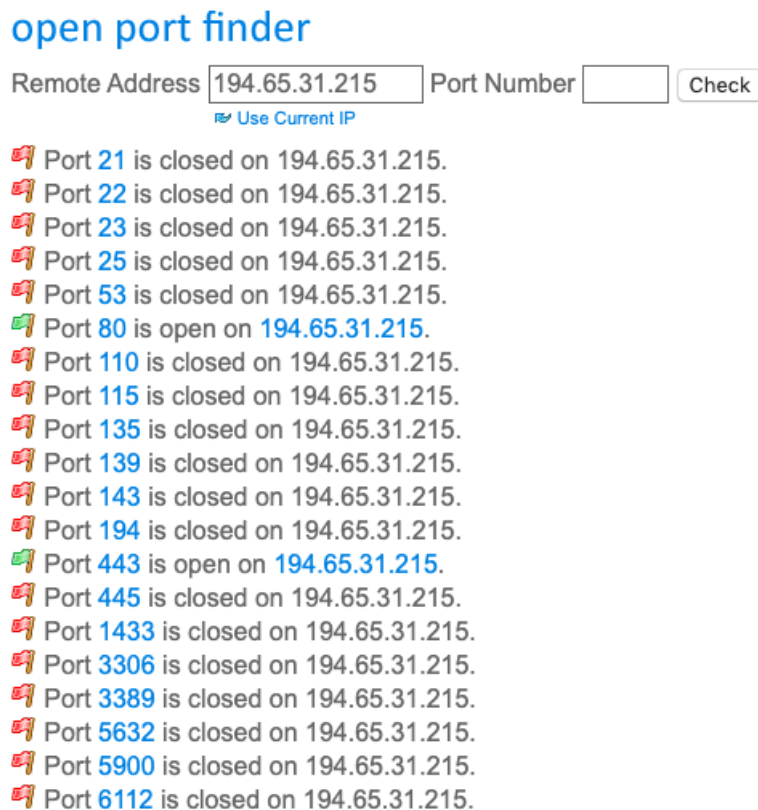


Figura 2. Exemplo de teste feito a portas do IPv4 correspondente a www.pingodoce.pt

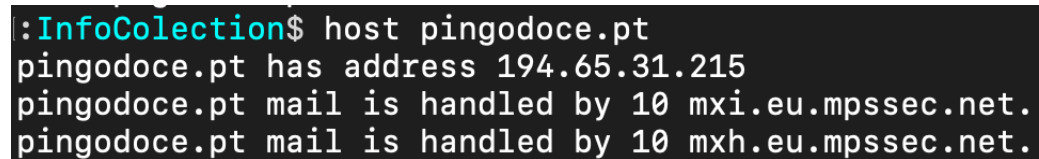
Portas testadas:

- FTP
- SSH
- TELNET
- SMTP
- DNS
- HTTP

- POP3
- SFTP
- RPC
- netBIOS
- IMAP
- IRC
- SSL
- SMB
- MSSQL
- MySQL
- RemoteDesktop
- PCAnywhere
- VNC
- Warcraft III

Com esta análise podemos concluir que tanto o HTTP como o SSL têm as respectivas portas abertas.

Determinar o endereço de email é uma forma de localizar a firewall da organização, para isso basta usar *host pingodoce.pt*. O resultado pode ser visto na figura abaixo.



```
:InfoCollection$ host pingodoce.pt
pingodoce.pt has address 194.65.31.215
pingodoce.pt mail is handled by 10 mxi.eu.mpssec.net.
pingodoce.pt mail is handled by 10 mxh.eu.mpssec.net.
```

Figura 3. Emails referentes a pingodoce.pt

Por fim, fazendo uso do nmap sobre o IP referente a pingodoce.pt obtemos as seguintes imagens.

manutenção de servidores, precavam-se contra possíveis ataques de DoS e em termos de acesso a informação sensível sobre a rede interna da empresa. No entanto peca na vertente da engenharia social, a informação de quem são os empregados é pública e estes não uma fonte de preocupação em termos de segurança visto que na maior parte das vezes estes são a porta de entrada para um sistema.

5 GamingReplay

A empresa especializa-se na venda/compra de artigos relacionados com videojogos desde consolas e videojogos para as mesmas mas também Merchandising. Está no mercado desde 2009 mas com experiência desde 2007 nesta área.

GamingReplay é uma marca comercializada em Portugal por:
SharingJourney, Lda.
 Candal Park - Fraction B-21
 Rua 28 de Janeiro,350
 4400-335 Vila Nova de Gaia

Pessoa colectiva n° 510650449 Matriculada na CRC de Loulé

Figura 6. Informação da Empresa

A marca é comercializada por *SharingJourney,Lda* como pode ser visto na figura 6 retirada do Website. Apesar de a Gamingreplay estar no mercado desde 2009 a empresa que a comercializa foi oficialmente criada a 21 de Junho de 2013.

5.1 Localização & Contactos

Esta pequena empresa tem duas lojas físicas localizadas em *Arrábida Shopping Piso 1 - Loja 166 - Vila Nova de Gaia* e em *Almada Fórum Piso 0 - Loja 1.112 - Almada* para além disso também gerem um Website que funciona como loja Online em <https://www.gamingreplay.pt>(Figura 7). Ainda sobre a loja online ainda pode descobrir-se um Código Postal associado (4400-275).

A primeira loja tem associado tanto um email lojaarrabida@gamingreplay.com como um telefone 224 103 675, o mesmo se aplica á segunda loja lojaalmada@gamingreplay.com - 265 414 909 e á loja online clientes@gamingreplay.com - 919 176 465.

Figura 7. Localização da Empresa

Loja 1 Arrábida Shopping Piso 1 - Loja 166 - Vila Nova de Gaia
Loja 2 Almada Fórum Piso 0 - Loja 1.112 - Almada
Loja 3 Loja Online https://www.gamingreplay.pt

5.2 Política de privacidade

A política de privacidade que consta na página da empresa está conforme o previsto no *Regulamento (UE) 2016/679* do Parlamento Europeu e do Conselho de 27 de Abril de 2016.

Os dados pessoais (nome, e-mail, telefone, morada) dos clientes são guardados pelo período de 2 anos desde o consentimento pelo mesmo. Caso o cliente usufrua de algum serviço da empresa o prazo será extendido para 5 anos. O utilizador tem o direito de realizar as seguintes operações indicadas na figura 8.

Figura 8. Operações do Cliente sobre os seus dados

Tem o direito de, sempre que quiser e gratuitamente, pedir à GAMINGREPLAY para:

- aceder aos dados que nos indicou
- pedir a retificação dos seus dados
- pedir o apagamento dos seus dados
- pedir a limitação do tratamento dos seus dados
- opor-se ao tratamento dos seus dados
- solicitar a portabilidade dos seus dados para entidade por si indicada. Note-se, porém, que caso exista norma ou obrigação legalmente imposta que se sobreponha a estes direitos, a GAMINGREPLAY responderá a impossibilidade de executar o pedido, indicando o respetivo fundamento.

5.3 Domínios Associados

O website *www.gamingreplay.com* é utilizado como a página principal do negócio, porém ao pesquisar os A records associados (Figura 9) a esse mesmo domínio encontramos o seguinte:

1. Os domínios que contem "media" redirecionam para a página principal. Possivelmente sejam vários servidores para prevenir ataques de Denial of Service.
2. O domínio começado por "phpma" corresponde a uma página administração de base de dados, mais especificamente corresponde a um software phpMyAdmin que permite gerir base de dados MySQL através da

Web. Para aceder a base de dados é necessário um par username/password.

3. O domínio webdisk.gamingreplay.com corresponde a um serviço de gestão de ficheiros usados pelo website requiere autenticação para aceder ao serviço
4. O domínio cpanel.gamingreplay.com diz respeito a um serviço de gestão do Website onde pode estar integrado o serviço anterior. Como os anteriores requiere autenticação.
5. O domínio webmail.gamingreplay.com tanto como o autodiscover.gamingreplay.com fornecem serviços de gestão de e-mail. O primeiro está integrado no Cpanel e o segundo é um serviço necessário para usar o Outlook Exchange.
6. O domínio gamingreplayserver.gamingreplay.com provavelmente diz respeito ao back-end da página. Encontra-se em Lisboa e a empresa responsável por esse IP é a *Claranet Portugal*.

Note-se que todos estes domínios excepto o último estão localizados no mesmo IPv4.

Figura 9. A records associados a Gamingreplay.com

```
media1.gamingreplay.com,94.46.135.139
www.media1.gamingreplay.com,94.46.135.139
media2.gamingreplay.com,94.46.135.139
www.media2.gamingreplay.com,94.46.135.139
media3.gamingreplay.com,94.46.135.139
www.media3.gamingreplay.com,94.46.135.139
phpma.gamingreplay.com,94.46.135.139
www.phpma.gamingreplay.com,94.46.135.139
webdisk.gamingreplay.com,94.46.135.139
cpanel.gamingreplay.com,94.46.135.139
webmail.gamingreplay.com,94.46.135.139
autodiscover.gamingreplay.com,94.46.135.139
gamingreplayserver.gamingreplay.com,80.172.235.82
```

Observando outros tipos de DNS records(Figura 10) pode concluir-se também que:

1. Os servidores DNS que estão responsáveis pelo domínio pertence a empresa linxisp sendo o ns1.linxisp.net o servidor primário.

2. No record TXT encontra-se dois IPs um corresponde ao IP associado ao Website.O outro corresponde a um serviço de Cloud da empresa *Almouroltec - Serviços Informática Internet, Lda.* Este formato de record Txt corresponde a um Sender Policy Framework ,isto é, os IPs que podem enviar emails através do domínio de forma a autenticar a origem do email e este não ser considerado como spam.

Figura 10. DNS records associados a Gamingreplay.com

gamingreplay.com.	14399	IN	TXT	"v=spf1 ip4:94.46.135.139 ip4:130.185.81.169 +a +mx +include:spf.xcloudsender.com -all"
gamingreplay.com.	14399	IN	MX	@ gamingreplay.com.
gamingreplay.com.	21599	IN	SOA	ns1.linxisp.net. suporte.linxisp.com. 2019060600 3600 1800 1209600 86400
gamingreplay.com.	21599	IN	NS	ns4.linxisp.net.
gamingreplay.com.	21599	IN	NS	ns2.linxisp.net.
gamingreplay.com.	21599	IN	NS	ns3.linxisp.net.
gamingreplay.com.	21599	IN	NS	ns1.linxisp.net.
gamingreplay.com.	14399	IN	A	94.46.135.139

Finalmente analisou-se um header do pedido HTTP(Figura 11) usado para aceder ao Website principal. Analisando o conteúdo do Header pode retirar-se que utilizam um servidor Apache e as cookies sao "escolhidas" pelo software PrestaShop.

O software Prestashop é utilizados para automatizar os processos de uma loja online.No entanto requiere que os utilizadores tenham instalado um servidor Web Apache 1.3 ou posterior, PHP 5 ou superior e o MySQL 5 ou superior.

Figura 11. HTTP Header de Gamingreplay.com

```
HTTP/1.1 200 OK
Date: Sat, 02 Nov 2019 19:00:47 GMT
Server: Apache
P3P: CP="IDC DSP COR CURA ADMa OUR IND PHY ONL COM STA"
Powered-By: PrestaShop
Set-Cookie: PrestaShop-0cd10abe556956d490dbba3e30e16990-j95X8K9UxIujojoYLqznoXLwHnlokD384kNsLMBi7mtPRjEAlahPqLIwgVK%2F4E0YIVny9tsQAKQTmGzH8YwVaD1U%2FVsKAY3nKkJPEHC7w58%3D0000075; expires=Sun, 03-Nov-2019 19:00:47 GMT; Max-Age=86399; path=/; domain=www.gamingreplay.com; secure; httponly
Content-Type: text/html; charset=utf-8
```

6 Estratégias para Ocultar Informação

As empresas devem utilizar algumas técnicas para diminuir a "pegada" digital. Seguidamente, enumerar-se-ão algumas possíveis soluções:

1. A informação disponibilizada nos Websites deve ser revista para evitar que dados sobre a segurança, tratamento de dados, tecnologia etc. sejam usados

pelos atacantes. É necessário ter em consideração os aspetos legais como de próprio funcionamento dos serviços da empresa.

2. As empresas que registam domínios oferecem serviços para ocultar os dados com e-mail, número de telemovel, etc. Impedindo o atacante de obter informação e pontos de ataques para realizar "Social Engineering" facilmente.
3. Restringir as transferências de Zona permitidas.
4. Configurar os Nameservers para só responder com informação de serviços ligados diretamente a Internet.
5. Implementar sistemas de prevenção de intrusos para evitar reconhecimento da rede da empresa.
6. Garantir que se têm ACLs robustas que não permitam o acesso a ficheiros ou a pastas confidenciais e sensíveis a alguém fora do sistema.