# 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 empresas visada, consultaram-se on 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 querys com os comandos dig e whois acerca dos servidores responsáveis pela footprint da empresa na internet. Para alé disso pode também ser consultado o site para obter informações que digam respeito ás tecnologias usadas em páginas antigas ou ao próprio código modificado. Neste são especificados os tipos de dados que se podem pretender obter com um ataque á empresa e como estes são tratados. Também são referidos contactos de telemóvel, telefone, emails e localizações consideradas pertinentes. No fim exibem-se querys feitas aos servidores e as respostas obtidas sendo prossecutidas por uma breve explicação.

**Palavras-chave:** wget · Whois · dig · pingodoce

# 1 Dados a roubar

Dados como nome, morada e número de contribuinte são mantidos pelo periodo 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.

## 1.1 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.

# 2 Autenticação - Facebook ou Google

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

# 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 engeniering":

  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

---

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:
dsiaccounts@jeronimo-martins.pt,dsiaccounts@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:
dsiaccounts@jeronimo-martins.pt,dsiaccounts@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 pais 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. O resultado segue em baixo.

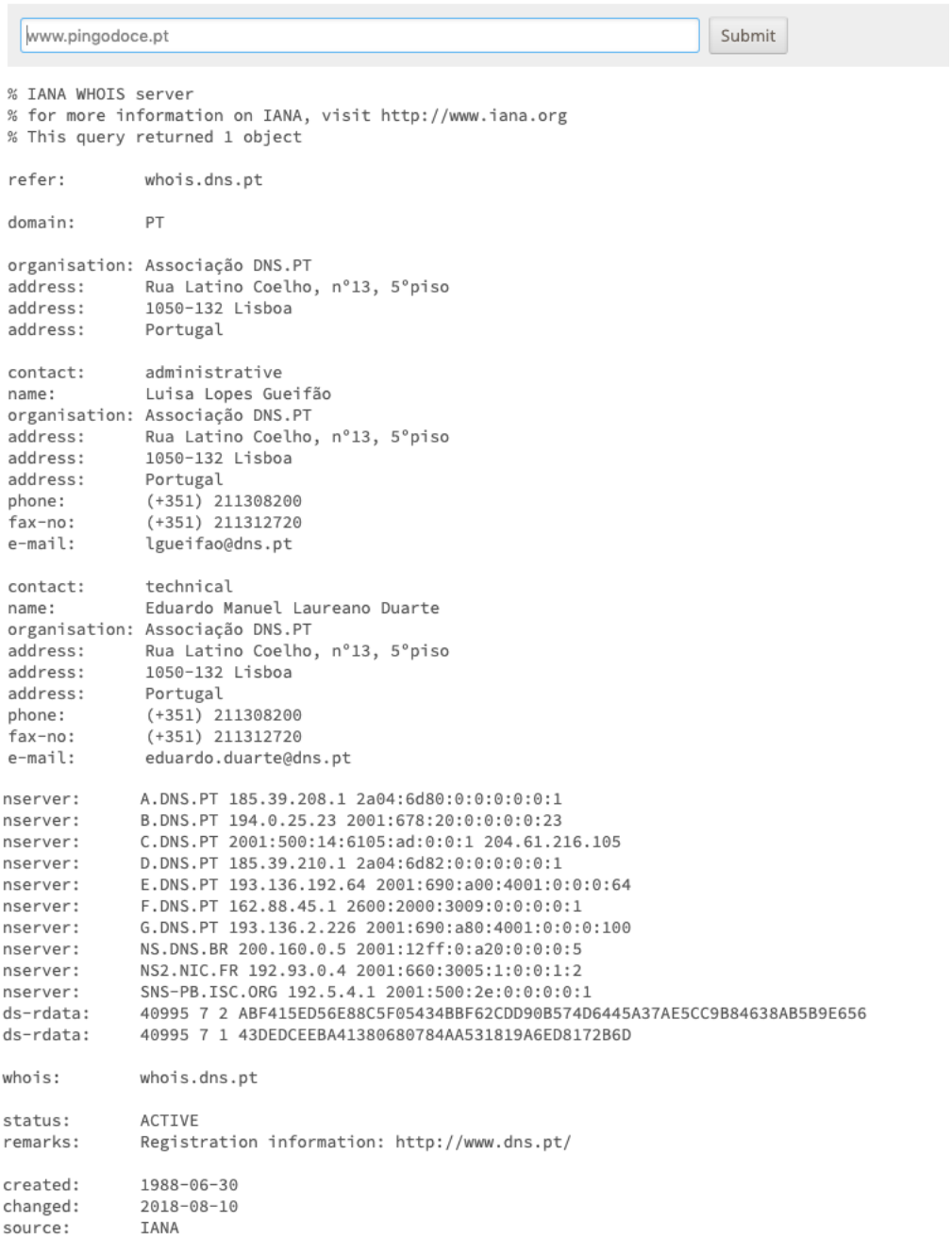


**Figura 1.** Dados do registador do site www.pingodoce.pt

Este resultado ....
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 seguinda bem como os respetivos resultados.

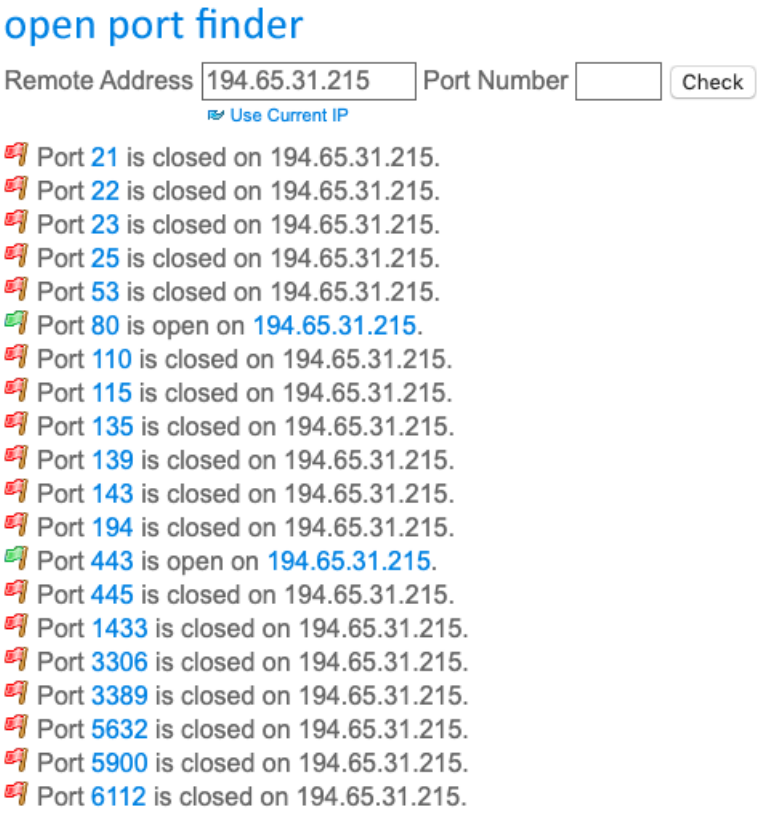


**Figura 2.** Exemplo de teste feito a portas do IPv4 correspondente a www.pingodoce.pt

**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 análize podemos concluir que tanto o HTTP como o SSL têm as respetivas portas abertas.